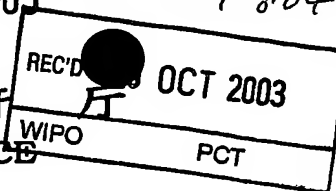


Reg'd PCT/PTO 09 MAR 2005 PCT/JB 03/11906

17.09.03

10/527072

本 国 特 許  
JAPAN PATENT OFFICE



*[Handwritten signature]*

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月19日

出 願 番 号

Application Number:

特願2002-273903

[ST.10/C]:

[JP2002-273903]

出 願 人

Applicant(s):

ソニー株式会社

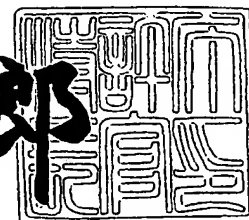
**PRIORITY  
DOCUMENT**

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年 6月18日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3047701

【書類名】 特許願  
 【整理番号】 0290632508  
 【提出日】 平成14年 9月19日  
 【あて先】 特許庁長官殿  
 【国際特許分類】 G06F 7/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
 内

【氏名】 大森 和雄

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
 内

【氏名】 本城 哲

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
 内

【氏名】 末吉 正弘

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
 内

【氏名】 花木 直文

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
 内

【氏名】 館野 啓

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理方法、そのプログラムおよびその装置

【特許請求の範囲】

【請求項 1】

鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第 1 の認証用データを保持する被認証手段と、前記鍵データを保持する認証手段とが行うデータ処理方法であって、

前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の工程と、

前記認証手段が、前記第 1 の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第 2 の認証用データを生成する第 2 の工程と、

前記被認証手段が前記第 1 の認証用データを用い、前記認証手段が前記第 2 の認証用データを用いて、認証を行う第 3 の工程と、

前記認証手段が、前記第 3 の工程の前記認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する第 4 の工程と

を有するデータ処理方法。

【請求項 2】

鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第 1 の認証用データを保持する被認証手段と、

前記鍵データを保持する認証手段と

を有し、

前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供し、

前記認証手段が、前記被認証手段から受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第 2 の認証用データを生成し、

前記被認証手段が前記第 1 の認証用データを用い、前記認証手段が前記第 2 の認証用データを用いて、認証を行い、

前記認証手段が、前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する

データ処理システム。

【請求項3】

所定の鍵データを保持する認証手段が、前記鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第1の認証用データを保持する被認証手段と認証を行うデータ処理方法であって、

前記鍵データを指定する鍵指定データを前記被認証手段から受ける第1の工程と、

前記第1の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証用データを生成する第2の工程と、

前記第2の工程で生成した前記第2の認証用データを用いて、前記第1の認証用データを認証に用いる前記被認証手段と前記認証を行う第3の工程と、

前記第3の工程の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する第4の工程と

を有するデータ処理方法。

【請求項4】

前記第4の工程において、前記鍵データに関連付けられた、前記被認証手段に許可された前記認証手段の機能、または前記認証手段が保持するデータへのアクセスを実行する

請求項3に記載のデータ処理方法。

【請求項5】

前記認証用データが異なる複数の前記鍵データを用いて生成されている場合に

前記第4の工程において、前記複数の鍵データにそれぞれ関連付けられた複数の処理を実行する

請求項3に記載のデータ処理方法。

【請求項 6】

前記第 4 の工程において、前記複数の鍵データにそれぞれ関連付けられた、前記認証手段の機能および前記認証手段が保持するデータへのアクセスを含む複数の処理を実行する

請求項 5 に記載のデータ処理方法。

【請求項 7】

前記第 4 の工程において、前記認証手段が複数のデータモジュールを前記データとして保持している場合に、単数の前記鍵データに関連付けられた、複数の前記データモジュールへのアクセスを実行する

請求項 3 に記載のデータ処理方法。

【請求項 8】

前記第 1 の工程において、前記第 1 の認証用データおよび前記鍵指定データを保持する集積回路から前記被認証手段の装置が読み出した前記鍵指定データを受ける

請求項 3 に記載のデータ処理方法。

【請求項 9】

前記第 1 の認証用データは、所定のデータを前記鍵データを用いて暗号化して生成されたデータである

請求項 3 に記載のデータ処理方法。

【請求項 10】

前記第 1 の認証用データは、前記所定のデータを前記鍵データを用いて暗号化して得られたデータを、管理元が管理する改竄防止鍵データをさらに用いて暗号化して生成されたデータである

請求項 9 に記載のデータ処理方法。

【請求項 11】

所定の鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第 1 の認証用データを保持する被認証手段と認証を行い、前記鍵データを保持するデータ処理装置であって、

前記被認証手段から、前記鍵データを指定する鍵指定データを入力する入力手

段と、

前記入力手段が受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証用データを生成し、当該第2の認証用データを用いて、前記第1の認証用データを認証に用いる前記被認証手段と前記認証を行う認証手段と、

前記認証手段が前記認証により前記第1の認証用データと前記第2の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する制御手段と

を有するデータ処理装置。

【請求項12】

所定の鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第1の認証用データを保持する被認証手段と認証を行い、前記所定の鍵データを保持するデータ処理装置が実行するプログラムであって、

前記鍵データを指定する鍵指定データを前記被認証手段から受ける第1の手順と、

前記第1の手順で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証用データを生成する第2の手順と、

前記第2の手順で生成した前記第2の認証用データを用いて、前記第1の認証用データを認証に用いる前記被認証手段と前記認証を行う第3の手順と、

前記第3の手順の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する第4の手順と

を有するプログラム。

【請求項13】

鍵データを保持する認証手段が、第1の認証用データを保持する被認証手段から指定された前記鍵データを用いて所定の生成手法を基に第2の認証用データを生成し、前記第2の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第1の認証用データと前記第2の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、

前記被認証手段が行うデータ処理方法であって、

前記所定の生成方法を基に前記第1の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第1の工程と、

前記第1の認証用データを用いて、前記認証手段と前記認証を行う第2の工程と、

前記第2の工程の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第3の工程と

を有するデータ処理方法。

【請求項14】

前記被認証手段は、所定の集積回路から前記第1の認証用データおよび前記鍵指定データを読み出して保持する

請求項13に記載のデータ処理方法。

【請求項15】

前記第3の工程において、前記鍵データに関連付けられた、前記被認証手段に許可された前記認証手段の機能を前記認証手段に実行させるか、または、前記認証手段が保持するデータへのアクセスを実行する

請求項13に記載のデータ処理方法。

【請求項16】

複数の前記認証手段からなるグループを規定した場合に、

前記第1の工程において、前記グループに対して前記鍵指定データを一括して提供し、

前記第3の工程において、前記グループに対して前記鍵データに関連付けられた処理を一括して行わせる

請求項13に記載のデータ処理方法。

【請求項17】

前記処理を行う前記認証手段に対応する画像を、前記認証手段の動作状態に応じて異なる複数のパターンを用いて表示する画面を提供する第4の工程

をさらに有する請求項13に記載のデータ処理方法。

【請求項18】



前記第 4 の工程において、前記第 2 の工程の認証により前記認証手段が、前記被認証手段の正当性を既に認めたか否かを識別可能なパターンで、前記認証手段に対応する画像を表示した前記画面を提供する

請求項 1 7 に記載のデータ処理方法。

【請求項 1 9】

鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて所定の生成手法を基に第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段を構成するデータ処理装置であって、

前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手段と、

前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の手段と、

前記第 2 の手段の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の手段と

を有するデータ処理装置。

【請求項 2 0】

鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて所定の生成手法を基に第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段を構成するデータ処理装置によって実行されるプログラムであって、

前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手順と、

前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の手順

と、

前記第 2 の手順の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の手順と

を有するプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、認証結果を基に所定の処理を行うデータ処理方法、そのプログラムおよびその装置に関する。

【0002】

【従来の技術】

認証手段が、被認証手段の正当性を確認した後に、当該被認証手段に許可された処理を実行するシステムがある。

このようなシステムでは、例えば、認証手段が、全ての被認証手段についての相互認証鍵データを保持し、それぞれの認証手段との間で、当該認証手段に対応する相互認証鍵データを選択して相互認証を行う。

そして、認証手段は、上記相互認証により、被認証手段の正当性を確認すると、管理テーブルなどを基に予め被認証手段に対して許可された処理を特定し、当該特定した処理を実行する。

【0003】

【発明が解決しようとする課題】

しかしながら、上述した従来のシステムでは、被認証手段は、全ての認証手段に対応した相互認証鍵データを保持する必要がある、相互認証鍵データの管理負担が大きいという問題がある。

また、上述した従来のシステムでは、相互認証とは別に、被認証手段に許可した処理を管理テーブルを基に特定する必要がある、管理テーブルの作成および管理などの負担が大きいという問題がある。

【0004】

本発明はかかる事情に鑑みてなされたものであり、その目的は、認証手段が被

認証手段を認証した後に、当該被認証手段に許可した処理を実行する場合に、認証手段の処理負担を軽減することを可能にするデータ処理方法、そのプログラムおよびその装置を提供することを目的とする。

## 【 0 0 0 5 】

## 【課題を解決するための手段】

上述した目的を達成するために、第 1 の発明のデータ処理方法は、鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第 1 の認証用データを保持する被認証手段と、前記鍵データを保持する認証手段とが行うデータ処理方法であって、前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の工程と、前記認証手段が、前記第 1 の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第 2 の認証用データを生成する第 2 の工程と、前記被認証手段が前記第 1 の認証用データを用い、前記認証手段が前記第 2 の認証用データを用いて、認証を行う第 3 の工程と、前記認証手段が、前記第 3 の工程の前記認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する第 4 の工程とを有する。

## 【 0 0 0 6 】

第 1 の発明のデータ処理方法の作用は以下のようなになる。

第 1 の工程において、前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供する。

次に、第 2 の工程において、前記認証手段が、前記第 1 の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第 2 の認証用データを生成する。

次に、第 3 の工程において、前記被認証手段が前記第 1 の認証用データを用い、前記認証手段が前記第 2 の認証用データを用いて、認証を行う。

次に、第 4 の工程において、前記認証手段が、前記第 3 の工程の前記認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する。

## 【 0 0 0 7 】

第2の発明のデータ処理システムは、鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第1の認証用データを保持する被認証手段と、前記鍵データを保持する認証手段とを有し、前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供し、前記認証手段が、前記被認証手段から受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証用データを生成し、前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記第2の認証用データを用いて、認証を行い、前記認証手段が、前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する。

## 【0008】

第2の発明のデータ処理システムの作用は以下のようになる。

まず、前記被認証手段が、前記鍵データを指定する鍵指定データを前記認証手段に提供する。

次に、前記認証手段が、前記第1の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証用データを生成する。

次に、前記被認証手段が前記第1の認証用データを用い、前記認証手段が前記第2の認証用データを用いて、認証を行う。

次に、前記認証手段が、前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断すると、前記鍵データに関連付けられた処理を実行する。

## 【0009】

第3の発明のデータ処理方法は、所定の鍵データを保持する認証手段が、前記鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第1の認証用データを保持する被認証手段と認証を行うデータ処理方法であって、前記鍵データを指定する鍵指定データを前記被認証手段から受ける第1の工程と、前記第1の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証用データを生成する第2の工程と、前記第2の工程で生成した前記第2の認証用データを用いて、前記第1の認証用データを認証に用いる前記被認証手段と前記認証を行う第3の工程と、前記第3の工程の前記認証に

より、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する第 4 の工程とを有する。

## 【 0 0 1 0 】

第 4 の発明のデータ処理装置は、所定の鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第 1 の認証用データを保持する被認証手段と認証を行い、前記鍵データを保持するデータ処理装置であって、前記被認証手段から、前記鍵データを指定する鍵指定データを入力する入力手段と、前記入力手段が受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第 2 の認証用データを生成し、当該第 2 の認証用データを用いて、前記第 1 の認証用データを認証に用いる前記被認証手段と前記認証を行う認証手段と、前記認証手段が前記認証により前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する制御手段とを有する。

## 【 0 0 1 1 】

第 5 の発明のプログラムは、所定の鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第 1 の認証用データを保持する被認証手段と認証を行い、前記所定の鍵データを保持するデータ処理装置が実行するプログラムであって、前記鍵データを指定する鍵指定データを前記被認証手段から受ける第 1 の手順と、前記第 1 の手順で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第 2 の認証用データを生成する第 2 の手順と、前記第 2 の手順で生成した前記第 2 の認証用データを用いて、前記第 1 の認証用データを認証に用いる前記被認証手段と前記認証を行う第 3 の手順と、前記第 3 の手順の前記認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであると判断した場合に、前記鍵データに関連付けられた処理を実行する第 4 の手順とを有する。

## 【 0 0 1 2 】

第 6 の発明のデータ処理方法は、鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて所定の生成

手法を基に第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段が行うデータ処理方法であって、前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の工程と、前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の工程と、前記第 2 の工程の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の工程とを有する。

## 【 0 0 1 3 】

第 7 の発明のデータ処理装置は、鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて所定の生成手法を基に第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段を構成するデータ処理装置であって、前記所定の生成方法を基に前記第 1 の認証用データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手段と、前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の手段と、前記第 2 の手段の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の手段とを有する。

## 【 0 0 1 4 】

第 8 の発明のプログラムは、鍵データを保持する認証手段が、第 1 の認証用データを保持する被認証手段から指定された前記鍵データを用いて所定の生成手法を基に第 2 の認証用データを生成し、前記第 2 の認証用データを用いて前記被認証手段と認証を行い、当該認証により、前記第 1 の認証用データと前記第 2 の認証用データとが同じであることを確認したことを条件に、前記鍵データに関連付けられた処理を行う場合に、前記被認証手段を構成するデータ処理装置によって実行されるプログラムであって、前記所定の生成方法を基に前記第 1 の認証用デ

ータを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第 1 の手順と、前記第 1 の認証用データを用いて、前記認証手段と前記認証を行う第 2 の手順と、前記第 2 の手順の認証の結果を基に、前記鍵データに関連付けられた処理を前記認証手段に行わせる第 3 の手順とを有する。

## 【 0 0 1 5 】

## 【発明の実施の形態】

以下、本発明の実施の形態を添付図面を参照して説明する。

図 1 は、本実施形態の通信システム 1 の全体構成図である。

図 1 に示すように、通信システム 1 は、店舗などに設置されたサーバ装置 2、IC カード 3、カードリーダー・ライタ 4、パーソナルコンピュータ 5、ASP (Application Service Provider) サーバ装置 19、SAM (Secure Application Module) ユニット 9 a, 9 b, . . . 、管理装置 20、IC モジュール 42 が内蔵された携帯通信装置 41 を用いて、インターネット 10 を介して通信を行って IC カード 3 あるいは携帯通信装置 41 を用いた決済処理などの手続き処理を行う。

## 【 0 0 1 6 】

通信システム 1 では、管理装置 20 および SAM ユニット 9 a, 9 b が本発明に対応した実施の形態に係わる処理を行う。

すなわち、管理装置 20 は、管理者等によって許可された所定の処理を SAM ユニット 9 a, 9 b に行わせるために用いる IC (本発明の集積回路) を内蔵したカード (例えば、後述するオナカードおよびユーザカード) を発行する処理を行う。これにより、相互認証に必要なデータを被認証手段に対して提供する。

また、管理装置 20 は、上記発行されたカードを管理者やユーザが用いて、SAM ユニット 9 a, 9 b との間で相互認証を行い、上記許可された所定の処理を SAM ユニット 9 a, 9 b に行わせる。

この場合に、管理装置 20 が本発明の被認証手段となり、SAM ユニット 9 a, 9 b が本発明の認証手段となる。

## 【 0 0 1 7 】

図 2 は、管理装置 20 の機能ブロック図である。

図2に示すように、管理装置20は、例えば、AP編集ツール51、管理ツール52、カードリーダー・ライタ53、ディスプレイ54、I/F55および操作部56を有する。

ここで、管理装置20が、第8の発明のデータ処理装置に対応し、I/F55は本発明の第1の手段、SAM管理機能部57が本発明の第2の手段および第3の手段に対応している。

【0018】

AP編集ツール51および管理ツール52は、データ処理装置でプログラム（第9の発明のプログラムに対応）を実行して実現してもよいし、電子回路（ハードウェア）によって実現してもよい。

管理ツール52は、例えば、SAM管理機能部57およびカード管理機能部58を有する。

カードリーダー・ライタ53は、以下に示す種々のカードのICとの間で、非接触式あるいは接触式でデータの授受を行う。

ディスプレイ54は、カード発行画面やAP管理画面を表示するために用いられる。

I/F55は、SAMユニット9a、9bとの間で、非接触式あるいは接触式でデータの授受を行う。

操作部56は、AP編集ツール51および管理ツール52に対して、指示やデータを入力ために用いられる。

【0019】

図3は、管理装置20が行う処理手順の概要を説明するためのフローチャートである。

ステップST1：

管理装置20は、管理者の操作に応じて、カード管理機能部58により、カードリーダー・ライタ53にセットされたデフォルトカード71を用いて、所定のデータが格納されたオーナカード72を作成する。また、オーナカード72を用いてユーザカード73を作成する。

すなわち、管理装置20は、SAMユニット9a、9b（本発明の認証手段）



に係わる処理のうち、オーナーカード72およびユーザカード73を用いた被認証手段に許可する処理に関連付けられた相互認証鍵データ（本発明の鍵データ）を用いて、後述するデバイス鍵データを所定の暗号化方法（本発明の所定の生成方法）で暗号化して、上記相互認証鍵データを復元困難な縮退鍵データ（本発明の第1の認証用データ）を生成する。

そして、管理装置20は、上記生成した縮退鍵データと、当該縮退鍵データの生成に用いた上記相互認証鍵データを指定する鍵指定データとを、オーナーカード72およびユーザカード73のIC（本発明の集積回路）に書き込む。

また、同様に、管理装置20は、トランスポートカード74およびAP暗号化カード75を作成する。

#### 【0020】

##### ステップST2：

オーナーカード72またはユーザカード73の使用者が、これらのカードを用いて、管理装置20を介して、当該使用者に権限が与えられた処理をSAMユニット9a、9bに行わせる場合に、上記使用者が管理装置20のカードリーダー・ライタ53に、オーナーカード72またはユーザカード73のICに記憶された上記鍵指定データを読み込ませる。

管理装置20のSAM管理機能部57は、当該読み込んだ鍵指定データをSAMユニット9a、9bに出力する。

#### 【0021】

##### ステップST3：

SAMユニット9a、9bが、上記鍵指定データが指定する相互認証鍵データを用いて、上記デバイス鍵データを上記所定の暗号化方法で暗号化して縮退鍵データ（本発明の第2の認証用データ）を生成する。

#### 【0022】

##### ステップST4：

SAM管理機能部57がカード72または73から読み出した縮退鍵データを用い、SAMユニット9a、9bが上記生成した縮退鍵データを用いて、認証を行う。

## 【0023】

ステップST5:

SAMユニット9a, 9bが、上記認証により、SAM管理機能部57とSAMユニット9a, 9bとが同じ上記縮退鍵データを保持していると判断すると、管理装置20からの指示に応じて、上記縮退鍵データの生成に用いられた単数または複数の相互認証鍵データに関連付けられた処理を実行する。

## -【0024】

図4は、図2に示すAP編集ツール51および管理ツール52に係わる処理において用いられるカードを説明するための図である。

図4に示すように、管理装置20の管理ツール52を用いて、SAMユニット9a, 9bにアクセスする場合に、オーナーカード72およびユーザカード73が用いられる。

また、AP編集ツール51で生成したAPパッケージファイルを管理ツール52に提供する場合に、AP暗号化カード75のICに記憶された暗号化鍵データを用いて、当該APパッケージファイルが暗号化される。

すなわち、図4に示すように、ユーザが、AP編集ツール51を用いて、SAMモジュール8内のアプリケーションプログラムAPを構成するアプリケーションエレメントデータAPEを作成する。

そして、AP編集ツール51が、単数または複数のアプリケーションエレメントデータAPEを含むAPパッケージファイルを作成し、これをAP暗号化カード75に格納された暗号鍵データを用いて暗号化して管理ツール52に提供する。

管理ツール52は、上述したように、SAMユニット9a, 9bと相互認証を行い、当該相互認証に用いた相互認証鍵データに関連付けて許可されたSAMユニット9a, 9b内のAP記憶領域に対して、AP編集ツール51から受けたAPパッケージファイルを書き込む。

また、トランスポートカード74は、SAMユニット9a, 9bが保持する鍵データなどのセキュリティに係わるデータを取り出して他の機器に転送したり、保存等するために用いられる。

## 【0025】

〔ICカード3および携帯通信装置41〕

図5は、ICカード3の機能ブロック図である。

図5に示すように、ICカード3は、メモリ50およびCPU51を備えたIC(Integrated Circuit)モジュール3aを有する。

メモリ50は、図6に示すように、クレジットカード会社などのサービス事業者15\_1が使用する記憶領域55\_1、サービス事業者15\_2が使用する記憶領域55\_2、並びにサービス事業者15\_3が使用する記憶領域55\_3を有する。

また、メモリ50は、記憶領域55\_1へのアクセス権限を判断するために用いられる鍵データ、記憶領域55\_2へのアクセス権限を判断するために用いられる鍵データ、並びに記憶領域55\_3へのアクセス権限を判断するために用いられる鍵データを記憶している。当該鍵データは、相互認証や、データの暗号化および復号などに用いられる。

また、メモリ50は、ICカード3あるいはICカード3のユーザの識別データを記憶している。

## 【0026】

携帯通信装置41は、携帯電話網およびインターネット10を介してASPサーバ装置19a、19bと通信を行う通信処理部43と、通信処理部43との間でデータ授受可能なICモジュール42とを有し、アンテナからインターネット10を介してSAMユニット9aと通信を行う。

ICモジュール42は、携帯通信装置41の通信処理部43とデータ授受を行う点を除いて、前述したICカード3のICモジュール3aと同じ機能を有している。

なお、携帯通信装置41を用いた処理は、ICカード3を用いた処理と同様に行われ、ICモジュール42を用いた処理はICモジュール3aを用いた処理と同様に行われるため、以下の説明では、ICカード3およびICモジュール3aを用いた処理について例示する。

## 【0027】

以下、SAMユニット9a、9bについて説明する。

図1に示すように、SAMユニット9a、9bは、外部メモリ7とSAMモジュール8とを有する。

ここで、SAMモジュール8は、半導体回路として実現してもよいし、筐体内に複数の回路を収容した装置として実現してもよい。

#### 【0028】

##### 〔SAMモジュール8のソフトウェア構成〕

SAMモジュール8は、図7に示すようなソフトウェア構成を有している。

図7に示すように、SAMモジュール8は、下層から上層に向けて、ハードウェアHW層、周辺HWに対応したRTOSカーネルなどを含めたドライバ層（OS層）、論理的にまとまった単位の処理を行う下位ハンドラ層、アプリケーション固有のライブラリなどをまとめた上位ハンドラ層およびAP層を順に有している。

ここで、AP層では、図1に示すクレジットカード会社などのサービス事業者15\_1、15\_2、15\_3によるICカード3を用いた手続きを規定したアプリケーションプログラムAP\_1、AP\_2、AP\_3が、外部メモリ7から読み出されて動作している。

AP層では、アプリケーションプログラムAP\_1、AP\_2、AP\_3相互間、並びに上位ハンドラ層との間にファイアウォールFWが設けられている。

#### 【0029】

##### 〔SAMモジュール8のハードウェア構成〕

図8は、SAMモジュール8のハードウェア構成、並びに外部メモリ7の記憶領域を説明するための図である。

図8に示すように、SAMモジュール8は、例えば、メモリI/F61、外部I/F62、メモリ63、認証部64およびCPU65を有し、これらがバス60を介して接続されている。

ここで、SAMモジュール8が、第4の発明のデータ処理装置に対応し、外部I/F62が本発明の入力手段、認証部64が本発明の認証手段、CPU65が本発明の制御手段にそれぞれ対応している。

また、SAMモジュール8が、第5の発明のデータ処理装置に対応し、以下に示す各手順を含むプログラムを実行して、その機能を実現してもよい。

## 【0030】

メモリI/F61は、外部メモリ7との間でデータ授受を行う。

外部I/F62は、図1に示すASPサーバ装置19a、19bおよび管理装置20との間で、データおよびコマンドの授受を行う。

メモリ63は、後述するSAMユニット9a、9bの相互認証などに用いられる種々の鍵データなどを記憶する。当該鍵データは、外部メモリ7のAP管理用記憶領域221に記憶されていてもよい。

認証部64は、後述する相互認証に係わる処理を行う。認証部64は、例えば、所定の鍵データを用いた暗号化および復号などを処理を行う。

CPU65は、SAMモジュール8の処理を統括して制御する。

CPU65は、後述するように、相互認証で正当な相手であることを確認すると、被認証手段に対して、後述する相互認証鍵データに関連付けられた処理を許可し、これを実行する。

SAMモジュール8による相互認証処理については、後に詳細に説明する。

## 【0031】

## 〔外部メモリ7〕

図8に示すように、外部メモリ7の記憶領域には、サービス事業者15\_\_1のアプリケーションプログラムAP\_\_1が記憶されるAP記憶領域220\_\_1（サービスAPリソース領域）、サービス事業者15\_\_2のアプリケーションプログラムAP\_\_2が記憶されるAP記憶領域220\_\_2、サービス事業者15\_\_3のアプリケーションプログラムAP\_\_3が記憶されるAP記憶領域220\_\_3、並びにSAMモジュール208の管理者が使用するAP管理用記憶領域221（シスエムAPリソース領域および製造者APリソース領域）がある。

## 【0032】

AP記憶領域220\_\_1に記憶されているアプリケーションプログラムAP\_\_1は、図9に示すように、後述する複数のアプリケーションエレメントデータAPE（本発明のデータモジュール）によって構成されている。AP記憶領域22

0\_\_1へのアクセスは、ファイアウォールFW\_\_1によって制限されている。

AP記憶領域220\_\_2に記憶されているアプリケーションプログラムAP\_\_2は、図9に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220\_\_2へのアクセスは、ファイアウォールFW\_\_2によって制限されている。

AP記憶領域220\_\_3に記憶されているアプリケーションプログラムAP\_\_3は、図9に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220\_\_3へのアクセスは、ファイアウォールFW\_\_3によって制限されている。

本実施形態では、上記アプリケーションエレメントデータAPEは、例えば、SAMユニット9aの外部から外部メモリ7にダウンロードされる最小単位である。各アプリケーションプログラムを構成するアプリケーションエレメントデータAPEの数は、対応するサービス事業者が任意に決定できる。

#### 【0033】

また、アプリケーションプログラムAP\_\_1, AP\_\_2, AP\_\_3は、例えば、それぞれ図1に示すパーソナルコンピュータ16\_\_1, 16\_\_2, 16\_\_3を用いて、サービス事業者15\_\_1, 15\_\_2, 15\_\_3によって作成され、SAMモジュール8を介して外部メモリ7にダウンロードされる。

#### 【0034】

なお、AP管理用記憶領域221に記憶されたプログラム、並びにデータも、上述したアプリケーションエレメントデータAPEを用いて構成されている。

#### 【0035】

図10は、上述したアプリケーションエレメントデータAPEを説明するための図である。

アプリケーションエレメントデータAPEは、図10に示すように、APEの属性(種別)を基に規定された分類を示すAPEタイプによって規定されたインスタンスを用いて構成される。

各インスタンスは、エレメントIDと、エレメントプロパティと、エレメントバージョンとによって規定されている。

APEタイプを基に、当該アプリケーションエレメントデータAPEが、サービスAP記憶領域220\_\_1, 220\_\_2, 220\_\_3およびAP管理用記憶領域221の何れに格納されるかが規定される。

サービスAP記憶領域220\_\_1は、各サービス事業者がアクセス可能なデータを記憶する。

なお、AP管理用記憶領域221は、システムの管理者がアクセス可能なデータを記憶するシステムAP記憶領域と、システムの製造者がアクセス可能なデータを記憶する製造者AP記憶領域とを有する。

また、サービスAP記憶領域220\_\_1, 220\_\_2, 220\_\_3およびAP管理用記憶領域221によって、AP記憶領域が構成される。

本実施形態では、上述したサービスAP記憶領域220\_\_1, 220\_\_2, 220\_\_3およびAP管理用記憶領域221の各々にはID (AP記憶領域ID) が割り当てられており、APEタイプ、インスタンス、並びにエレメントバージョンの各々には識別用の番号 (APEタイプ番号、インスタンス番号、並びにエレメントバージョン番号) が割り当てられている。

#### 【0036】

図11は、APEタイプの一例を説明するための図である。

図11に示すように、APEタイプには、ICシステム鍵データ、ICエリア鍵データ、ICサービス鍵データ、IC縮退鍵データ、IC鍵変更パッケージ、IC発行鍵パッケージ、IC拡張発行鍵パッケージ、ICエリア登録鍵パッケージ、ICエリア削除鍵パッケージ、ICサービス登録鍵パッケージ、ICサービス削除鍵パッケージ、ICメモリ分割鍵パッケージ、ICメモリ分割素鍵パッケージ、障害記録ファイル、相互認証用鍵、パッケージ鍵、ネガリストおよびサービスデータテンポラリファイルがある。

各APEタイプには、APEタイプ番号が割り当てられている。

#### 【0037】

以下、図11に示すAPEタイプのうち一部を説明する。

ICシステム鍵データ、ICエリア鍵データ、ICサービス鍵データおよびIC縮退鍵データは、ICカード3およびICモジュール42のメモリ50に対し

てのデータの読み書き操作に用いられるカードアクセス鍵データである。

相互認証用鍵データ同一SAM内にあるAP間相互認証にも使用される。SAM相互認証用鍵データとは、対応するアプリケーションエレメントデータAPEを同一SAM内の他のAPまたは他のSAMからアクセスする際に用いられる鍵データである。

#### 【0038】

ICメモリ分割用鍵パッケージは、サービス事業者がICカード3を用いたサービスの運用開始前に、外部メモリ7やICカード3のメモリの記憶領域を分割するために使用するデータである。

ICエリア登録鍵パッケージは、サービス事業者がICカード3を用いたサービスの運用開始前に、ICカード3のメモリの記憶領域にエリア登録を行う場合に使用するデータである。

ICエリア削除用鍵パッケージは、カードアクセス鍵データからSAM内部で自動生成が可能なパッケージである。

ICサービス登録用鍵パッケージは、サービス事業者がICカード3を用いたサービスの運用開始前に、外部メモリ7のアプリケーションエレメントデータAPEを登録するために用いられる。

ICサービス削除用鍵パッケージは、外部メモリ7に登録されているアプリケーションエレメントデータAPEを削除するために用いられる。

#### 【0039】

##### 〔オーナーカード72およびユーザカード73の作成〕

図12は、オーナーカード72およびユーザカード73の作成手順を説明するためのフローチャートである。

図12は、図3に示すステップST1、ST2を詳細に示すものである。

##### ステップST11：

例えば、管理者が、オーナーカード72を作成する場合には、オーナーカード72の使用者に許可するSAMユニット9a、9bに係わる処理を選択する。

また、管理者等が、ユーザカード73を作成する場合に、ユーザカード73の使用者に許可するSAMユニット9a、9bに係わる処理を選択する。



SAMユニット9a, 9bに係わる処理には、例えば、SAMユニット9a, 9bが提供する機能を実行する処理、またはSAMユニット9a, 9bが保持するデータ（例えば、アプリケーションエレメントデータAPE）へのアクセスなどがある。

## 【0040】

## ステップST12:

管理者等が、ステップST11で選択した処理に関連付けられた相互認証鍵データを選択して、管理装置20のカード管理機能部58に入力あるいは指定する。

当該相互認証鍵データについては後に詳細に説明する。

## 【0041】

## ステップST13:

管理装置20のカード管理機能部58が、ステップST12で選択された単数または複数の相互認証鍵データを用いて後述する縮退処理方法（本発明の所定の生成方法）を基に縮退鍵データを生成する。

当該縮退処理については後に詳細に説明する。

## 【0042】

## ステップST14:

管理装置20のカード管理機能部58が、ステップST13で縮退鍵データの生成に用いた、相互認証鍵データを識別する相互認証コードを示す鍵指定データを生成する。

当該鍵指定データは、オーナーカード72またはユーザカード73の利用者が取得した、SAMユニット9a, 9bに係わる処理の実行権限を示すデータとなる。

## 【0043】

## ステップST15:

管理装置20のカード管理機能部58が、ステップST13で生成した縮退鍵データと、ステップST14で生成した鍵指定データとを、オーナーカード72またはユーザカード73のICに書き込む。

## 【0044】

ステップST16:

管理装置20のカード管理機能部58が、ステップST13の縮退鍵データの生成に用いた、相互認証鍵データをSAMユニット9a, 9bに登録する。

## 【0045】

以下、上述した図12に示すステップST12で選択する対象となる相互認証鍵データについて説明する。

図13は、図12に示すステップST12で選択する対象となる相互認証鍵データを説明するための図である。

図13に示すように、当該相互認証鍵データには、例えば、デバイス鍵データ、ターミネーション鍵データ、製造設定サービス相互認証鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、相互認証サービス相互認証鍵データ、AP記憶領域管理サービス相互認証鍵データ、サービスAP記憶領域相互認証鍵データ、システムAP記憶領域相互認証鍵データ、並びに製造者AP記憶領域相互認証鍵データがある。

## 【0046】

また、図13および図14に示すように、相互認証鍵データの相互認証コードが、図14に示すように、図10を用いて説明したAP記憶領域ID、エレメントタイプ番号、エレメントインスタンス番号およびエレメントバージョン番号から構成される。

## 【0047】

以下、上述した図12に示すステップST14で生成する鍵指定データについて説明する。

当該鍵指定データは、上述した複数の相互認証鍵データの相互認証コードを用いて構成される、相互認証コードリストである。

図15は、鍵指定データの一例を説明するための図である。

図12のステップST12で、例えば、図13に示すデバイス鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、AP記憶領域管理サービス相互認証鍵データ、サービスAP記憶領域相互認証鍵データ、

並びにターミネーション鍵データが選択された場合には、図15(A)に示すように、当該選択された全ての相互認証鍵データの相互認証コードを示す鍵指定データが生成される。

図12に示すステップST13において、図15(A)に示す相互認証コードの相互認証鍵データを用いて縮退鍵データが生成された場合には、当該縮退鍵データを用いたSAMユニット9a, 9bとの相互認証により、管理装置20に対して、図15(B)に示すように、機器管理サービス、通信管理サービス、ICサービス(ICカード3およびICモジュール421に関するサービス)、相互認証サービスおよびAP記憶領域管理サービスが許可される。

#### 【0048】

このように、本実施形態では、SAMユニット9a, 9bの機能と、SAMユニット9a, 9bが保持するデータ(例えば、アプリケーションエレメントデータAPE)へのアクセスを含む複数の処理にそれぞれ関連付けられた相互認証鍵データを用いて縮退鍵データを生成できる。

これにより、単数の縮退鍵データを用いた相互認証により、SAMユニット9a, 9bが、SAMユニット9a, 9bの機能と、SAMユニット9a, 9bが保持するデータへのアクセスとの双方について、それらを被認証手段に対して許可するか否かを一括して判断できる。

そして、SAMユニット9a, 9bは、被認証手段が正当であると認証した場合に、当該被認証手段の指示に応じて、上記相互認証鍵データに関連付けられた所定の機能に係わる処理を実行すると共に、SAMユニット9a, 9bが保持するデータへの上記被認証手段からのアクセスを許可する。

#### 【0049】

以下、図12に示すステップST13の縮退処理方法について説明する。

図16は、当該縮退処理方法を説明するためのフローチャートである。

ステップST21:

管理装置20のカード管理機能部58が、デバイス鍵データをメッセージとし、図12に示すステップST12で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用い

て、デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、ステップ S T 1 2 で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部 5 8 は、上記中間鍵データを用いて次のステップ S T 2 2 の処理を行う。

一方、ステップ S T 1 2 で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データが 2 以上の場合には、カード管理機能部 5 8 は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。

カード管理機能部 5 8 は、ステップ S T 1 2 で選択されたデバイス鍵データおよびターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップ S T 2 2 の処理に進む。

ステップ S T 2 2 :

カード管理機能部 5 8 が、ステップ S T 2 1 で得られた中間鍵データをメッセージとして、ターミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ターミネーション鍵データは、改竄防止鍵データであり、管理者のみが保持している。

これにより、管理者以外の者が、不正に縮退鍵データを改竄することを防止できる。

【 0 0 5 0 】

以下、上述したターミネーション鍵データとして、管理者（オーナー）のみが所有するオーナーターミネーション鍵データと、上記管理者から権限を与えられたユーザが所有するユーザターミネーション鍵データとを用いて、所定の縮退処理方法で、縮退鍵データを生成する場合を説明する。

図 1 7 は、当該縮退処理方法を説明するためのフローチャートである。

図 1 7 において、ステップ S T 3 1, S 3 2 の処理は、ターミネーション鍵データとして、上記オーナーターミネーション鍵データを用いる点を除いて、図 1 6 を用いて説明したステップ S T 2 1, 2 2 の処理と同じである。

ステップST32で生成された縮退鍵データは、ユーザターミネーション鍵データを与えられたユーザが、拡張できるという意味で拡張可能な縮退鍵データである。

#### ステップST33：

管理装置20のカード管理機能部58が、オーナーが生成した拡張可能縮退鍵データをメッセージとし、ユーザが選択したユーザターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部58は、上記中間鍵データを用いて次のステップST22の処理を行う。

一方、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが2以上の場合には、カード管理機能部58は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。

カード管理機能部58は、上記選択されたユーザターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップST34の処理に進む。

#### ステップST34：

カード管理機能部58が、ステップST33で得られた中間鍵データをメッセージとして、ユーザターミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ユーザターミネーション鍵データは、改竄防止鍵データであり、上記オーナーおよび上記ユーザのみが保持している。

これにより、上記オーナーおよび上記ユーザ以外の者が、不正に縮退鍵データを改竄することを防止できる。

#### 【0051】

図17に示す処理によって生成された縮退鍵データは、図18に示すような階層で相互認証鍵が暗号化されたものになる。

#### 【0052】

また、本実施形態では、単数の相互認証鍵データ（例えば、図 1 3 に示すサービス、システム、製造者 A P 記憶領域相互認証鍵データ）に、複数のアプリケーションエレメントデータ A P E を関連付けてもよい。

これにより、縮退鍵データを用いた認証により、S A M ユニット 9 a, 9 b が、単数の相互認証鍵データに関連付けられたアプリケーションエレメントデータ A P E へのアクセスを許可するか否かを一括して判断できる。

例えば、図 1 9 では、相互認証鍵データ 5 0 0 に、アプリケーションエレメントデータ A P E のインスタンス a のパーミッション C と、インスタンス b のパーミッション B とが関連付けられている。そのため、相互認証鍵データ 5 0 0 を縮退した縮退鍵データを用いた認証が成功すれば、S A M ユニット 9 a, 9 b がインスタンス a, b の双方へのアクセスを許可する。

#### 【 0 0 5 3 】

また、本実施形態では、図 1 3 を用いた説明した相互認証鍵データの全てである一部について、図 2 0 に示すように、オンライン相互認証鍵データ M K 1 とオフライン相互認証鍵データ M K 2 とをペアで用いるようにしてもよい。

この場合には、相互認証を行う場合にはオンライン相互認証鍵データ M K 1 を用い、相互認証を行った相手とはデータ授受を行う場合には、それに対応するオフライン相互認証鍵データ M K 2 を用いて授受するデータを暗号化する。

これにより、仮にオンライン相互認証鍵データ M K 1 が不正に他人に取得された場合でも、被認証手段と認証手段とで授受するデータはオフライン相互認証鍵データ M K 2 で暗号化されているため、その情報が不正に漏れることを防止できる。

#### 【 0 0 5 4 】

以下、例えば、図 3 に示すステップ S T 3 などで行われる管理装置 2 0 の S A M 管理機能部 5 7 と S A M ユニット 9 a, 9 b との間の相互認証について説明する。

この場合に、管理装置 2 0 が被認証手段となり、S A M ユニット 9 a, 9 b が認証手段となる。

図 2 1 および図 2 2 は、管理装置 2 0 の S A M 管理機能部 5 7 と S A M ユニッ

ト 9 a との間の相互認証について説明するためのフローチャートである。

SAMユニット 9 b についても、以下に示す SAMユニット 9 a の場合と同じである。

【0055】

ステップ ST 5 1 :

先ず、管理者またはユーザが、オーナカード 7 2 またはユーザカード 7 3 を、カードリーダー・ライタ 5 3 にセットする。

そして、オーナカード 7 2 およびユーザカード 7 3 に記憶された縮退鍵データ K a (本発明の第 1 の認証用データ) および鍵指定データが、管理装置 2 0 の SAM管理機能部 5 7 に読み込まれる。

SAM管理機能部 5 7 が、乱数 R a を発生する。

【0056】

ステップ ST 5 2 :

SAM管理機能部 5 7 が、ステップ ST 5 1 で読み込んだ縮退鍵データ K a を用いて、ステップ ST 5 1 で生成した乱数 R a を、暗号化アルゴリズム 1 で暗号化してデータ R a' を生成する。

ステップ ST 5 3 :

SAM管理機能部 5 7 が、ステップ ST 5 1 で読み込んだ鍵指定データと、ステップ ST 5 2 で生成したデータ R a' とを SAMユニット 9 a に出力する。

SAMユニット 9 a は、図 8 に示す外部 I/F 6 2 を介して、当該鍵指定データおよびデータ R a' を入力して、これをメモリ 6 3 に格納する。

【0057】

ステップ ST 5 4 :

SAMユニット 9 a の認証部 6 4 が、メモリ 6 3 あるいは外部メモリ 7 に記憶された相互認証鍵データのなかから、ステップ ST 5 3 で入力した鍵指定データが示す相互認証鍵データを特定する。

ステップ ST 5 5 :

SAMユニット 9 a の認証部 6 4 が、ステップ ST 5 4 で特定した相互認証鍵データを用いて、図 1 6 あるいは図 1 7 を用いて前述した縮退処理を行って縮退

鍵データK bを生成する。

ステップST 56:

SAMユニット9 aの認証部64が、ステップST 55で生成した縮退鍵データK bを用いて、上記暗号化アルゴリズム1に対応した復号アルゴリズム1で、ステップST 53で入力したデータR a'を復号して乱数R aを生成する。

【0058】

ステップST 57:

SAMユニット9 aの認証部64が、上記縮退鍵データK bを用いて、暗号化アルゴリズム2で、ステップST 56で生成した乱数R aを暗号化して、データR a' 'を生成する。

ステップST 58:

SAMユニット9 aの認証部64が、乱数R bを生成する。

【0059】

ステップST 59:

SAMユニット9 aの認証部64が、上記縮退鍵データK bを用いて、ステップST 58で生成した乱数R bを、暗号化アルゴリズム2で暗号化してデータR b'を生成する。

ステップST 60:

SAMユニット9 aの認証部64が、ステップST 57で生成したデータR a' 'と、ステップST 59で生成したデータR b' 'とを管理装置20に出力する。

【0060】

ステップST 61:

管理装置20のSAM管理機能部57が、縮退鍵データK aを用いて、上記暗号化アルゴリズム2に対応した復号アルゴリズム2で、ステップST 60で入力したデータR a' 'およびR b' 'を復号してデータR a, R bを生成する。

ステップST 62:

管理装置20のSAM管理機能部57が、ステップST 51で生成した乱数R aと、ステップST 61で生成したデータR aとを比較する。



そして、SAM管理機能部57が、上記比較と結果が同じであることを示す場合に、SAMユニット9aが保持する上記縮退鍵データKbが、SAM管理機能部57が保持する上記縮退鍵データKaと同じであり、SAMユニット9aが正当な認証手段であると認証する。

#### 【0061】

ステップST63：

管理装置20のSAM管理機能部57が、縮退鍵データKaを用いて、暗号化アルゴリズム1で、ステップST61で生成したデータRbを暗号化して、データRb' 'を生成する。

ステップST64：

管理装置20のSAM管理機能部57が、ステップST63で生成したデータRb' 'をSAMユニット9aに出力する。

#### 【0062】

ステップST65：

SAMユニット9aの認証部64が、縮退鍵データKbを用いて、ステップST64で入力したデータRb' 'を、復号アルゴリズム1で復号してデータRbを生成する。

ステップST66：

SAMユニット9aの認証部64が、ステップST58で生成した乱数Rbと、ステップST65で生成したデータRbとを比較する。

そして、認証部64が、上記比較と結果が同じであることを示す場合に、SAMユニット9aが保持する上記縮退鍵データKbが、SAM管理機能部57が保持する上記縮退鍵データKaと同じであり、SAM管理機能部57が正当な被認証手段であると認証する。

#### 【0063】

以下、図21および図22を用いて説明した相互認証の結果を基に、SAMユニット9a、9bが行う処理を説明する。

図23は、SAMユニット9a、9bの処理を説明するための図である。

ステップST71：

図 8 に示す SAM ユニット 9 a, 9 b の CPU 65 が、図 22 に示すステップ ST 66 において、認証部 64 が認証手段が正当であると認証したか否かを判断し、正当であると認証したと判断した場合にはステップ ST 72 の処理に進み、そうでない場合には処理を終了する（すなわち、処理に係わる権限を有しないと判断し、処理を実行しない）。

## 【0064】

ステップ ST 72 :

SAM ユニット 9 a, 9 b の CPU 65 が、図 21 に示すステップ ST 54 で特定した相互認証鍵データに関連付けられた処理を実行する。これによって、被認証手段が要求する所定のサービスが提供される。すなわち、SAM ユニット 9 a, 9 b が、被認証手段が所定の権限を有すると判断し、当該権限について許可した処理を実行する。

## 【0065】

以下、図 2 および図 4 を用いて説明した管理装置 20 に関する各種のカードの発行に用いられる画面を説明する。

管理者等が、図 2 に示す操作部 56 を操作して、管理ツール 52 の操作画面表示を指示すると、例えば、図 24 に示すように、SAM 管理画面 750 がディスプレイ 54 に表示される。

SAM 管理画面 750 には、ツールバーに管理ツール用カードの作成指示用の画像 751 が表示されている。

また、SAM 管理画面 750 には、SAM ネットワークに接続された SAM のネットワーク構成を示す画像 752 が表示されている。

ユーザが、SAM 管理画面 750 上で画像 751 を例えば操作部 56 のマウスなどで指定すると、画像 753 が表示される。

画像 753 には、オーナーカードの作成、ユーザカードの作成、AP 暗号化カードの作成、トランスポートカードの作成を指示する画像が表示される。

## 【0066】

以下、画像 751 に示される各カードの作成を指示した場合の画面を説明する。

先ず、オーナカード作成の画面を説明する。

図24に示す画像751上のオーナカードの作成を上記マウスで管理者が指示すると、図2に示すカード管理機能部58が、図25に示すオーナカード作成画面760をディスプレイ54に表示する。

オーナカード作成画面760には、利用サービス選択画像761、サービスAP記憶領域指定画像762、システムAP領域指定画像763、デバイス／ターミネーション鍵指定画像764、並びに指定確定指示画像765が表示される。

#### 【0067】

利用サービス選択画像761は、例えば、作成するオーナカード72に許可するサービスの内容を選択するための画像である。

サービスAP記憶領域指定画像762は、作成するオーナカード72を用いたサービスAP記憶領域へのアクセスに対して許可する形態を選択するための画像である。

システムAP記憶領域指定画像763は、作成するオーナカード72を用いたシステムAP記憶領域へのアクセスに対して許可する形態を選択するための画像である。

デバイス／ターミネーション鍵指定画像764は、オーナカード72の作成に用いるデバイス鍵データおよびターミネーション鍵データを指定する画像である。

指定確定指示画像765は、上記指定した内容を確定させる指示を入力するための画像である。

#### 【0068】

管理者は、オーナカード作成画面760上で必要な項目の指定を完了すると、上記マウスなどで指定確定指示画像765を指定する。

これにより、図26に示すカードセット指示画面770がディスプレイ54に表示される。

オーナカード72の作成時には、カードセット指示画面770は、デフォルトカード71をセットする旨を指示する。

そして、管理者は、デフォルトカード71のICのデータをカードリーダー・ラ

イタ 53 に読み取らせる。

SAM管理機能部 57 は、デフォルトカード 71 の正当性を確認すると、オーナーカード作成画面 760 上で管理者が選択したサービス等に関連付けられた相互認証鍵データを選択する。当該選択が、図 12 を用いて説明したステップ ST 12 の選択に対応する。

#### 【0069】

次に、ユーザカード作成の画面を説明する。

図 24 に示す画像 751 上のユーザカードの作成を上記マウスで管理者が指示すると、図 2 に示すカード管理機能部 58 が、図 27 に示すユーザカード作成画面 780 をディスプレイ 54 に表示する。

ユーザカード作成画面 780 には、利用サービス選択画像 781、サービス AP 記憶領域指定画像 782、システム AP 領域指定画像 783、デバイス／ターミネーション鍵指定画像 784、並びに指定確定指示画像 785 が表示される。

#### 【0070】

利用サービス選択画像 781 は、例えば、作成するユーザカード 73 に許可するサービスの内容を選択するための画像である。

サービス AP 記憶領域指定画像 782 は、作成するユーザカード 73 を用いたサービス AP 記憶領域へのアクセスに対して許可する形態を選択するための画像である。

システム AP 記憶領域指定画像 783 は、作成するユーザカード 73 を用いたシステム AP 記憶領域へのアクセスに対して許可する形態を選択するための画像である。

デバイス／ターミネーション鍵指定画像 784 は、ユーザカード 73 の作成に用いるデバイス鍵データおよびターミネーション鍵データを指定する画像である。

指定確定指示画像 785 は、上記指定した内容を確定させる指示を入力するための画像である。

#### 【0071】

管理者は、オーナーカード作成画面 780 上で必要な項目の指定を完了すると、

上記マウスなどで指定確定指示画像 785 を指定する。

これにより、図 26 に示すカードセット指示画面 770 がディスプレイ 54 に表示される。

ユーザカード 73 の作成時には、カードセット指示画面 770 は、オーナカード 72 をセットする旨を指示する。

そして、管理者は、オーナカード 72 の IC のデータをカードリーダー・ライター 53 に読み取らせる。

SAM 管理機能部 57 は、オーナカード 72 の正当性を確認すると、ユーザカード作成画面 780 上で管理者が選択したサービス等に関連付けられた相互認証鍵データを選択する。当該選択が、図 12 を用いて説明したステップ ST12 の選択に対応する。

#### 【0072】

次に、AP 暗号化カード作成の画面を説明する。

図 24 に示す画像 751 上の AP 暗号化カードの作成を上記マウスで管理者が指示すると、図 2 に示すカード管理機能部 58 が、図 28 に示す AP 暗号化カード作成画面 790 をディスプレイ 54 に表示する。

AP 暗号化カード作成画面 790 には、利用サービス選択画像 791、サービス AP 記憶領域指定画像 792、システム AP 領域指定画像 793、デバイス／ターミネーション鍵指定画像 794、並びに指定確定指示画像 795 が表示される。

#### 【0073】

利用サービス選択画像 791 は、例えば、作成する AP 暗号化カード 75 に許可するサービスの内容を選択するための画像である。

サービス AP 記憶領域指定画像 792 は、作成する AP 暗号化カード 75 を用いたサービス AP 記憶領域へのアクセスに対して許可する形態を選択するための画像である。

システム AP 記憶領域指定画像 793 は、作成する AP 暗号化カード 75 を用いたシステム AP 記憶領域へのアクセスに対して許可する形態を選択するための画像である。

デバイス／ターミネーション鍵指定画像 794 は、AP 暗号化カード 75 の作成に用いるデバイス鍵データおよびターミネーション鍵データを指定する画像である。

指定確定指示画像 795 は、上記指定した内容を確定させる指示を入力するための画像である。

#### 【0074】

管理者は、AP 暗号化カード作成画面 790 上で必要な項目の指定を完了すると、上記マウスなどで指定確定指示画像 795 を指定する。

これにより、図 26 に示すカードセット指示画面 770 がディスプレイ 54 に表示される。

AP 暗号化カード 75 の作成時には、カードセット指示画面 770 は、例えば、オーナカード 72 をセットする旨を指示する。

そして、管理者は、オーナカード 72 の IC のデータをカードリーダー・ライター 53 に読み取らせる。

SAM 管理機能部 57 は、オーナカード 72 の正当性を確認すると、AP 暗号化カード作成画面 790 上で管理者が選択したサービス等に関連付けられた相互認証鍵データを選択する。当該選択が、図 12 を用いて説明したステップ ST12 の選択に対応する。

#### 【0075】

次に、トランスポートカード作成の画面を説明する。

図 24 に示す画像 751 上のトランスポートカードの作成を上記マウスで管理者が指示すると、図 2 に示すカード管理機能部 58 が、図 29 に示すトランスポートカード作成画面 800 をディスプレイ 54 に表示する。

トランスポートカード作成画面 800 は、データの搬送の対象として許可する SAM の IP アドレス、AP 記憶領域、アプリケーションエレメントデータ APE の APE タイプ、インスタンス番号およびバージョンを指定する画像を表示する。

カード管理機能部 58 は、トランスポートカード作成画面 800 上で指定された情報を基に、SAM ユニット 9a, 9b の記憶領域内のアクセスが許可された

データに関連付けられた相互認証鍵データを縮退して縮退鍵データを生成し、これをトランスポートカード74に書き込む。

#### 【0076】

上述したように、SAMユニット9a, 9bが提供する処理等を機能的に示した画面を基に、その機能を管理者等が、選択して各種のカードを発行することで、当該処理に実際に用いられる相互認証鍵データなどを、管理者に具体的に明示することなく、管理者が自らの意向に合った権限を持つカードを発行できる。これにより、SAMユニット9a, 9bのセキュリティに係わる情報が漏れることを回避できる。

#### 【0077】

以下、図2に示す管理ツール52のSAM管理機能部57が提供するSAM管理画面を説明する。

図30は、SAM管理画面1001を説明するための図である。

管理者等が、図2に示す操作部56を操作して、管理ツール52にSAM管理画面表示指示を認証要求先すると、例えば、図30に示すSAM管理画面1001がディスプレイ54に表示される。

図30に示すように、SAM管理画面1001は、メニュー・バー1002、SAMツリー領域1003、属性情報表示領域1004、詳細情報表示領域1005およびコンソール領域1006を有する。

メニュー・バー1002は、図2に示すカード管理機能部58の各種操作を指定するために用いられる。

当該操作には、ファイル操作、SAMコマンド操作、管理ツール用カード操作、コンソールログ操作およびヘルプ操作などがある。

#### 【0078】

SAMツリー領域1003には、SAM管理機能部57で操作するSAM（SAMユニット9a, 9b）と、そのSAMが属するグループが表示される。

ユーザは、SAMツリー領域1003上で、操作対象となるSAMを選択する。

属性情報表示領域1004には、SAMツリー領域1003で選択したSAM

やグループの情報が表示される。

詳細情報表示領域1005には、SAMツリー領域1003で選択したSAMやグループ内の各種情報の一覧が表示される。

コンソール領域1006には、SAMに対する各種操作の情報および結果が表示される。

#### 【0079】

図31は、SAMツリー領域1003の表示内容の一例を示す画面を説明するための図である。

図31に示すように、SAMツリー領域1003には、SAM管理機能部57で操作するSAMと、そのSAMが属するグループ等を示す種々のアイコンが表示される。

図32は、SAMツリー領域1003に表示されるアイコンを説明するための図である。

図32に示すように、SAMツリー領域1003に表示されるアイコンには、物体やデータを示すものとして、SAMネットワーク、グループ（SAMの集合体）、SAM（1台のSAM）、AP記憶領域、APEタイプ、インスタンスのアイコンがある。

また、SAMの状態を示すアイコンとして、SAMがサービスが開始されていない状態であることを示す「STANBY」、SAMが通常状態であることを示す「READY」、相互認証済の接続状態であることを示す「READY」、他の接続が完了するのを待っている状態であることを示す「SINGLE CONNECTION WAIT」、管理ツール52のみが接続していることを示す「SINGLE CONNECTION」などのアイコンがある。

このように、SAMツリー領域1003には、SAMに対応する画像を、SAMの動作状態に応じて異なる複数のパターンを用いて表示する。

これにより、ユーザは、SAMの状態を容易に特定できる。

また、SAMツリー領域1003には、SAMに対応する画像、当該SAMが相互認証済であるか、すなわち、被認証手段の正当性を既に認めたか否かを識別可能なパターンで表示するため、各SAMが相互認証を終えたか否かをユーザが



容易に特定できる。

#### 【0080】

図33は、SAMネットワーク画面1010を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でSAMネットワークのアイコンを指定すると、図33に示すSAMネットワーク画面1010がディスプレイ54に表示される。

SAMネットワーク画面1010には、SAMネットワークに接続されたSAMのIPアドレス、ポートおよび状態と、グループとについての情報が表示される。

#### 【0081】

図34は、グループ画面1020を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でグループのアイコンを指定すると、図34に示すグループ画面1020がディスプレイ54に表示される。

グループ画面1020には、指定されたグループに属するSAMのIPアドレス、ポートおよび状態についての情報が表示される。

#### 【0082】

図35は、SAM画面1030を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でSAMのアイコンを指定すると、図35に示すSAM画面1030がディスプレイ54に表示される。

SAM画面1030には、指定されたSAMのAP記憶領域のID、並びに、そのAP記憶領域の用途についての情報が表示される。

#### 【0083】

図36は、AP記憶領域画面1040を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でAP記憶領域のアイコンを指定すると、図36に示すAP記憶領域画面1040がディスプレイ54に表示される。

AP記憶領域画面1040には、指定されたAP記憶領域のAPEタイプの番

号、APEタイプの種類についての情報が表示される。

【0084】

図37は、APEタイプ画面1050を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でAPEタイプのアイコンを指定すると、図37に示すAPEタイプ画面1050がディスプレイ54に表示される。

APEタイプ画面1050には、指定されたAPEタイプを用いて構成されるインスタンスの番号、システムコード、エリア/サービスコードなどについての情報が表示される。

【0085】

図38は、インスタンス画面1060を説明するための図である。

図31に示すSAMツリー領域1003上で、ユーザがマウス等でインスタンスのアイコンを指定すると、図38に示すインスタンス画面1060がディスプレイ54に表示される。

インスタンス画面1060には、指定されたインスタンスの動作状態、記憶領域、ICサービス鍵およびインスタンス番号などの情報が表示される。

【0086】

図39は、図30に示すメニュー・バー1002のSAMコマンドを指定した場合の画面である。

図30に示すメニュー・バー1002上で、ユーザがマウス等でSAMコマンドのアイコンを指定すると、図39に示すSAMコマンド画面1070がディスプレイ54に表示される。

SAMコマンド画面1070には、SAMについての操作である、通信管理、AP記憶領域管理、ログ記録、ネガリスト、製造設定などの文字画像が表示されている。

ここで、ユーザが、通信管理を指定すると、ステータス取得、サービス開始、アクティベーションコード変更、シングルコネクション開始、コネクション切断などの文字画像が表示される。

ユーザは、これらの文字画像を指定することで、SAMに対しての操作を行う

## 【0087】

図40は、図30に示すSAM管理画面1001上でSAMのグループを作成する場合を説明するための図である。

図40に示すように、SAM管理画面1001上のSAMツリー領域1003のSAM管理の文字画像上で、ユーザがマウスなどで右クリックを行うと、操作画面1100が表示される。

操作画面1100には、SAMのグループ作成、SAMの追加およびSAMの最新状態を取得するなどの指示を行うための文字画像が表示される。

ユーザは、例えば、SAMのグループ作成の文字画像をマウスなどで指定することで、選択した複数のSAMからなるグループを規定することができる。

その場合に、SAM管理機能部57から、グループに鍵指定データを出力する指示を出すだけで、当該グループに属する全てのSAM（SAMユニット9a，9b）に対して、当該鍵指定データが一括して提供される。

また、SAM管理機能部57からの指示に応じて、当該グループに属する全てのSAMに対して、SAM管理機能部57が保持する縮退鍵データに対応した相互認証データに関連付けられた処理を一括して行わせることができる。

## 【0088】

以下、図2に示すAP編集ツール51が提供するAP記憶領域エディタについて説明する。

図41は、AP記憶領域エディタ画面1200を説明するための図である。

図41に示すように、AP記憶領域エディタ画面1200は、編集の対象とするAP記憶領域に格納されたアプリケーションエレメントデータAPEのAPEタイプおよびインスタンス番号を表示する。

また、AP記憶領域エディタ画面1200には、追加を示すアイコン1210、削除を示すアイコン1220、編集を示すアイコン1230が表示されている。

ユーザがマウスなどでアイコン1210を指定すると、当該AP記憶領域に対してのインスタンスの追加処理が行われる。

また、アイコン1210を指定すると、当該AP記憶領域に記憶されているインスタンスの削除処理が行われる。

また、アイコン1210を指定すると、当該AP記憶領域に記憶されているインスタンスの編集処理が行われる。

#### 【0089】

図42は、アプリケーションエレメントデータAPEのパッケージの追加を行うための画面1300を説明するための図である。

画面1300には、エレメントの作成、バージョンの追加の何れを行うかを指定する欄1301と、APEタイプを選択する欄1302と、インスタンス番号を指定する欄1303がある。

ユーザは、欄1301、1302および1303に追加するパッケージに関する情報を入力する。

これにより、AP編集ツール51が、自動的にエレメントパッケージの追加処理を行う。

#### 【0090】

図43は、アプリケーションエレメントデータAPEの作成を行うための画面1400を説明するための図である。

図42に示す画面1300上で所定の情報を入力して、画像1304を指定すると、図43に示すAPE作成画面1400が表示される。

APE作成画面1400には、作成対象とするアプリケーションエレメントデータAPEのタイプ、そのインスタンスの番号が表示される。

また、APE作成画面1400には、タグを指定する欄1401、使用バージョン数を指定する欄1402、エレメント取得の可否を指定する欄1403、データ自動生成の可否を指定する欄1404、並びにエレメント削除を指定する欄1405が表示される。

また、作成対象のアプリケーションエレメントデータAPEに関連付けられる各種の相互認証鍵データなどの属性情報名や値などを指定する欄1406が表示される。

#### 【0091】

図44は、アプリケーションエレメントデータAPEのバージョン追加を行うための画面1500を説明するための図である。

図42に示す画面1300上で、欄1301でバージョン追加を指定し、所定の情報を入力して、画像1304を指定すると、図44に示すAPEバージョン追加画面1500が表示される。

APEバージョン追加画面1500には、作成対象とするアプリケーションエレメントデータAPEのタイプ、そのインスタンスの番号が表示される。

また、APEバージョン追加画面1500には、エレメントバージョンを指定する欄1501、鍵データ入力方法を指定する欄1502、並びにエレメントデータの項目名および値を指定する欄1503が表示される。

#### 【0092】

上述した図42～図44に示す画面を用いて、アプリケーションエレメントデータAPEの作成およびバージョン追加を行うと、図45に示すように、AP記憶領域エディタ画面1200には、作成および追加したアプリケーションエレメントデータAPEに関する情報が欄1240に表示される。

#### 【0093】

以上説明したように、管理装置20によれば、図12および図16等を用いて説明したように、SAMユニット9a、9bに係わる処理に関連付けられた複数の相互認証鍵データを用いて縮退処理を行い、縮退鍵データを生成する。

そして、オーナーカード72やユーザカード73に、当該縮退鍵データ、並びにその生成に用いた相互認証鍵データを特定するための鍵指定データを書き込む。

また、オーナーカード72等を用いた管理装置20とSAMユニット9a、9bとの間で、図21～図23を用いた相互認証を行うことで、SAMユニット9aが管理装置20から受けた鍵指定データを基に縮退鍵データを生成し、当該縮退鍵データが管理装置20が保持するものと一致した場合に、被認証手段である管理装置20の正当性を確認できる。

また、その確認と共に、鍵指定データによって指定された相互認証鍵データに関連付けられた処理を、管理装置20に許可された処理であると判断できる。

そのため、認証手段であるSAMユニット9a、9bは、従来のように全ての

被認証手段（例えば、オーナーカード 7 2 およびユーザカード 7 3 を用いた管理装置 2 0 等）に対応した相互認証鍵データを保持する必要がなく、しかも、被認証手段に許可した処理を管理テーブルで管理する必要もなく、処理負担が軽減される。

#### 【0 0 9 4】

本発明は上述した実施形態には限定されない。

本発明は、例えば、オーナーカード 7 2、ユーザカード 7 3、トランスポートカード 7 4 および A P 暗号化カード 7 5 の何れかのカードの I C に、そのカードの使用者の生体情報を記憶させ、S A M ユニット 9 a、9 b が、上述した相互認証と共に、当該カードに記憶された生体情報をさらに用いて、その使用者の正当性を認証してもよい。

#### 【0 0 9 5】

例えば、上述した実施形態では、S A M ユニット 9 a、9 b が管理装置 2 0 と相互認証を行う場合を例示したが、S A M ユニット 9 a、9 b が A S P サーバ装置 1 9 a、1 9 b や他の S A M ユニットなどの被認証手段と認証を行ってもよい。この場合には、当該被認証手段が、上述した縮退鍵データおよび鍵指定データを保持する。

また、上述した実施形態では、オーナーカード 7 2 およびユーザカード 7 3 が、上述した縮退鍵データおよび鍵指定データを保持する場合を例示したが、その他の携帯装置などに、これらのデータを保持させてもよい。

#### 【0 0 9 6】

##### 【発明の効果】

以上説明したように、本発明によれば、認証手段が被認証手段を認証した後に、当該被認証手段に許可した処理を実行する場合に、認証手段の処理負担を軽減することを可能にするデータ処理方法、そのプログラムおよびその装置を提供することができる。

##### 【図面の簡単な説明】

##### 【図 1】

図 1 は、本発明の実施形態の通信システムの全体構成図である。

【図 2】

図 2 は、図 1 に示す管理装置の機能ブロック図である。

【図 3】

図 3 は、図 2 に示す管理装置が行う処理手順の概要を説明するためのフローチャートである。

【図 4】

図 4 は、図 2 に示す A P 編集ツールおよび管理ツールに係わる処理において用いられるカードを説明するための図である。

【図 5】

図 5 は、図 1 に示す I C カードの機能ブロック図である。

【図 6】

図 6 は、図 5 に示すメモリに記憶されたデータを説明するための図である。

【図 7】

図 7 は、図 1 に示す S A M モジュールのソフトウェア構成を説明するための図である。

【図 8】

図 8 は、図 1 に示す S A M モジュールのハードウェア構成、並びに外部メモリ 7 の記憶領域を説明するための図である。

【図 9】

図 9 は、図 8 に示す A P 記憶領域を説明するための図である。

【図 10】

図 10 は、アプリケーションエレメントデータを説明するための図である。

【図 11】

図 11 は、アプリケーションエレメントデータ A P E のタイプを説明するための図である。

【図 12】

図 12 は、オーナカードおよびユーザカードの作成手順を説明するためのフローチャートである。

【図 13】

図13は、相互認証鍵データを説明するための図である。

【図14】

図14は、相互認証コードを説明するための図である。

【図15】

図15は、相互認証鍵データとサービスとの関係を説明するための図である。

【図16】

図16は、縮退鍵データの生成方法を説明するための図である。

【図17】

図17は、縮退鍵データのその他の生成方法を説明するための図である。

【図18】

図18は、縮退鍵データの暗号化の階層を説明するための図である。

【図19】

図19は、縮退鍵データの特性の一例を説明するための図である。

【図20】

図20は、相互認証鍵データの使用形態の一例を説明するための図である。

【図21】

図21は、図1に示す管理装置のSAM管理機能部とSAMユニットとの間の相互認証について説明するためのフローチャートである。

【図22】

図22は、図1に示す管理装置のSAM管理機能部とSAMユニットとの間の相互認証について説明するための図21の続きのフローチャートである。

【図23】

図23は、SAMユニットの処理を説明するためのフローチャートである。

【図24】

図24は、図2および図4を用いて説明した管理装置に関係する各種のカードの発行に用いられる画面を説明するための図である。

【図25】

図25は、オーナーカードの作成用画面を説明するための図である。

【図26】



図 26 は、カード要求画面を説明するための図である。

【図 27】

図 27 は、ユーザカードの作成用画面を説明するための図である。

【図 28】

図 28 は、AP暗号化カードの作成用画面を説明するための図である。

【図 29】

図 29 は、トランスポートカードの作成用画面を説明するための図である。

【図 30】

図 30 は、SAM管理画面を説明するための図である。

【図 31】

図 31 は、図 30 に示す SAM ツリー領域の表示内容の一例を示す画面を説明するための図である。

【図 32】

図 32 は、図 30 に示す SAM ツリー領域に表示されるアイコンを説明するための図である。

【図 33】

図 33 は、SAM ネットワーク画面を説明するための図である。

【図 34】

図 34 は、グループ画面を説明するための図である。

【図 35】

図 35 は、SAM 画面を説明するための図である。

【図 36】

図 36 は、AP 記憶領域画面を説明するための図である。

【図 37】

図 37 は、APE タイプ画面を説明するための図である。

【図 38】

図 38 は、インスタンス画面を説明するための図である。

【図 39】

図 39 は、図 30 に示すメニュー・バーの SAM コマンドを指定した場合の画

面である。

【図 4 0】

図 4 0 は、図 3 0 に示す SAM 管理画面上で SAM のグループを作成する場合を説明するための図である。

【図 4 1】

図 4 1 は、AP 記憶領域エディタ画面を説明するための図である。

【図 4 2】

図 4 2 は、アプリケーションエレメントデータ A P E のパッケージの追加を行うための画面を説明するための図である。

【図 4 3】

図 4 3 は、アプリケーションエレメントデータ A P E の作成を行うための画面を説明するための図である。

【図 4 4】

図 4 4 は、アプリケーションエレメントデータ A P E のバージョン追加を行うための画面を説明するための図である。

【図 4 5】

図 4 5 は、一連の処理を経た後の AP 記憶領域エディタ画面を説明するための図である。

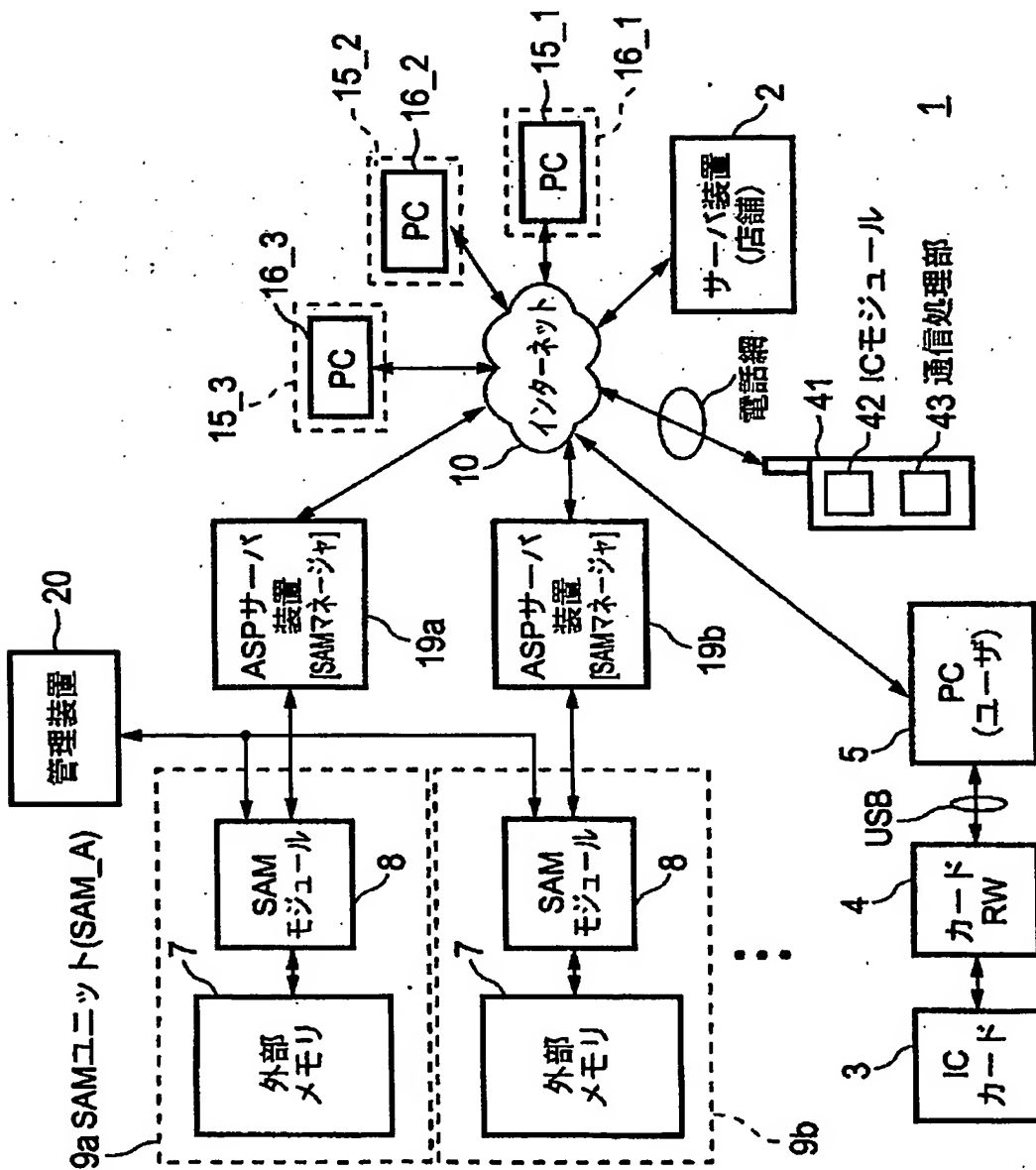
【符号の説明】

1…通信システム、2…サーバ装置、3…ICカード、4…カードRW、6…PC、7…外部メモリ、8…SAMモジュール、9a, 9b…SAMユニット、19a, 19b…ASPサーバ装置、20…管理装置、51…AP編集ツール、52…管理ツール、53…カードリーダー・ライター、54…ディスプレイ、55…I/F、56…操作部、57…SAM管理機能部、58…カード管理機能部、61…メモリI/F、62…外部I/F、63…メモリ、64…認証部、65…CPU、71…デフォルトカード、72…オーナーカード、73…ユーザカード、74…トランスポートカード、75…AP暗号化カード

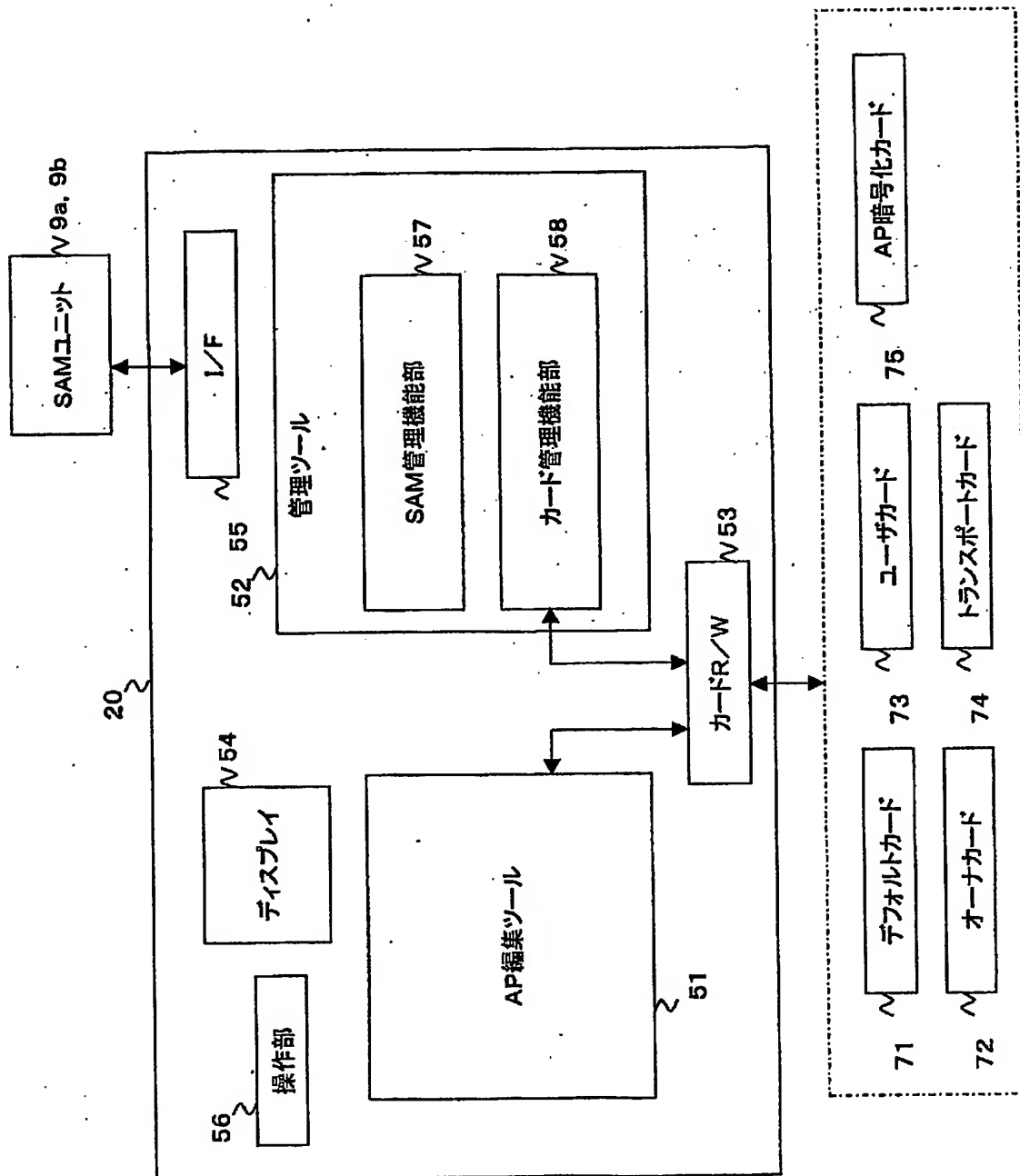
【書類名】

図面

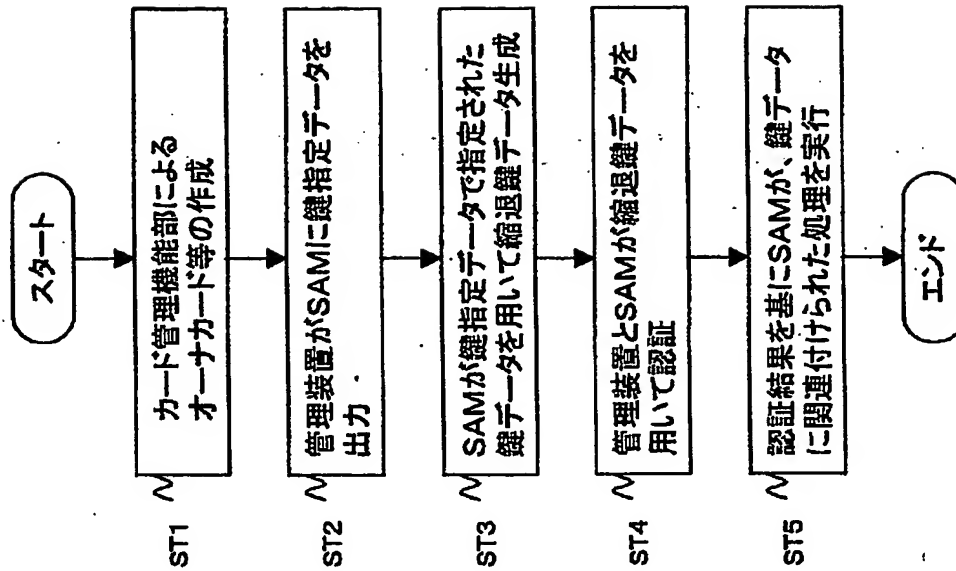
【図 1】



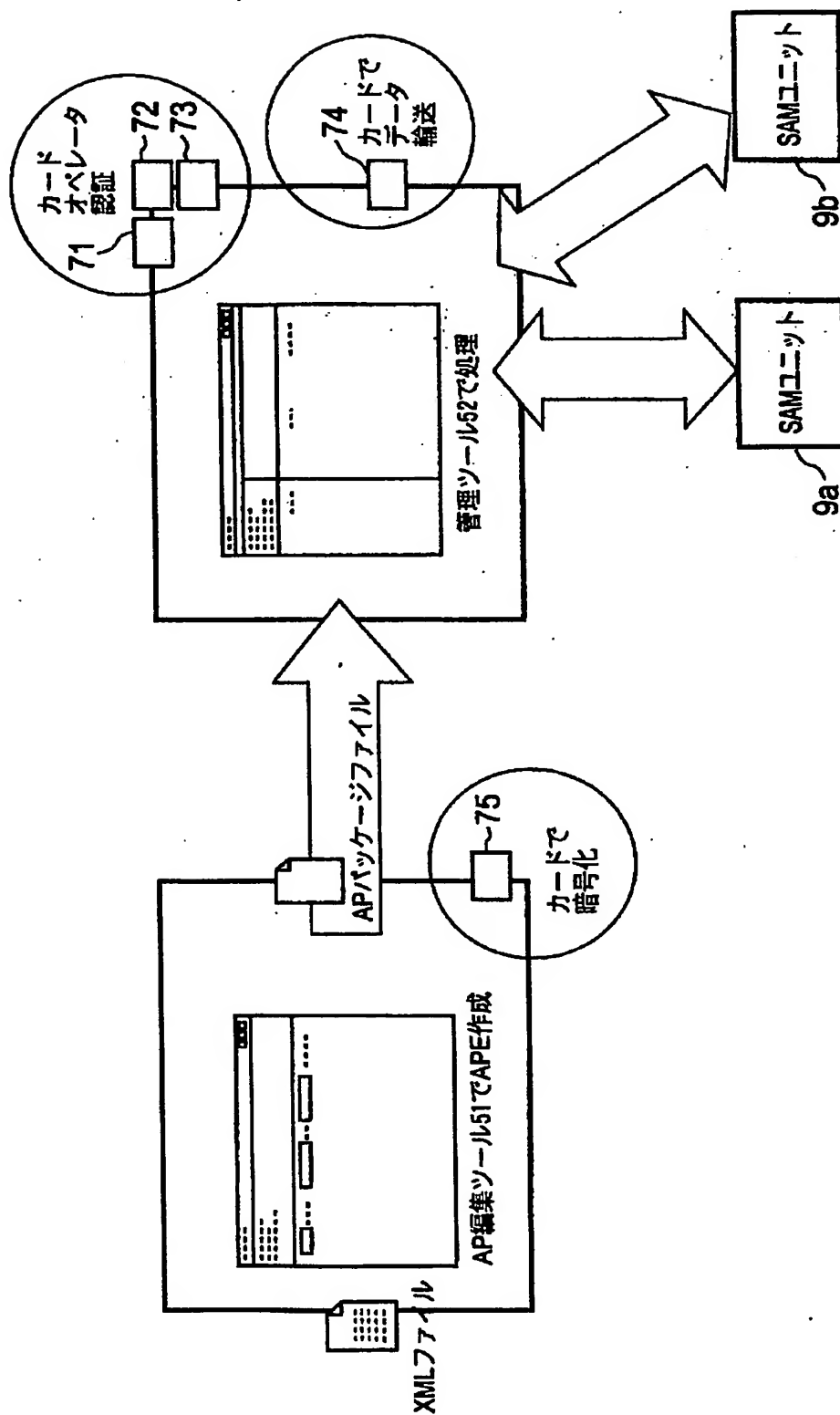
【図2】



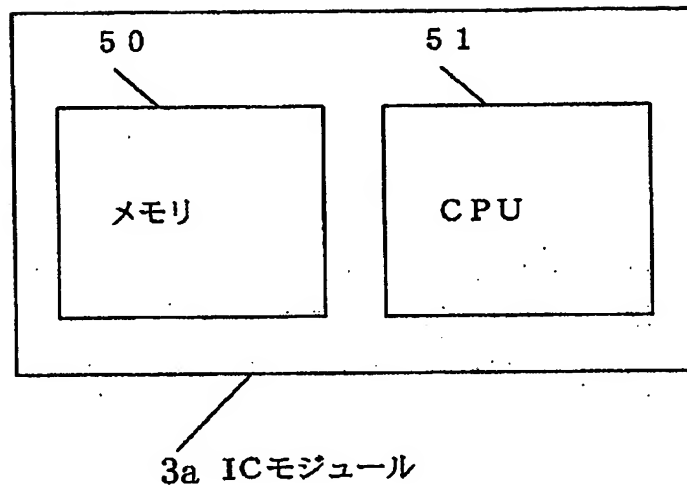
【図 3】



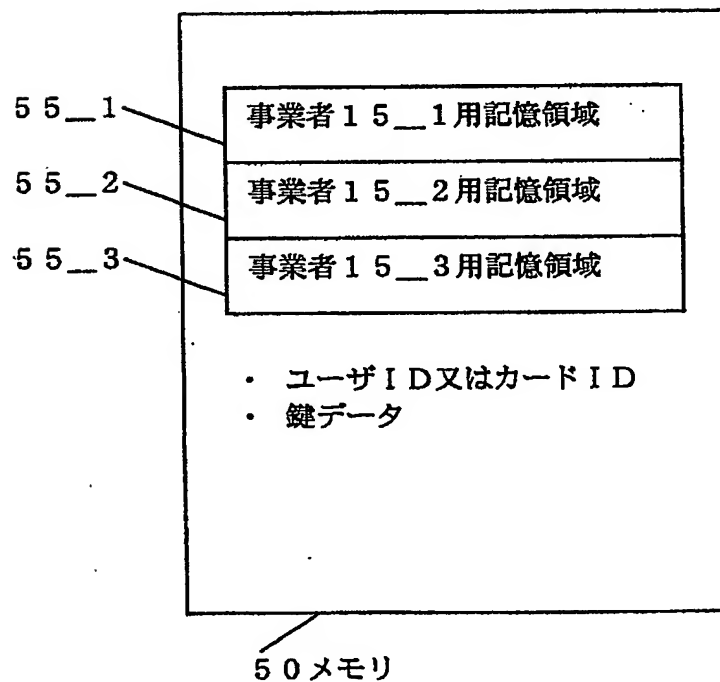
【図4】



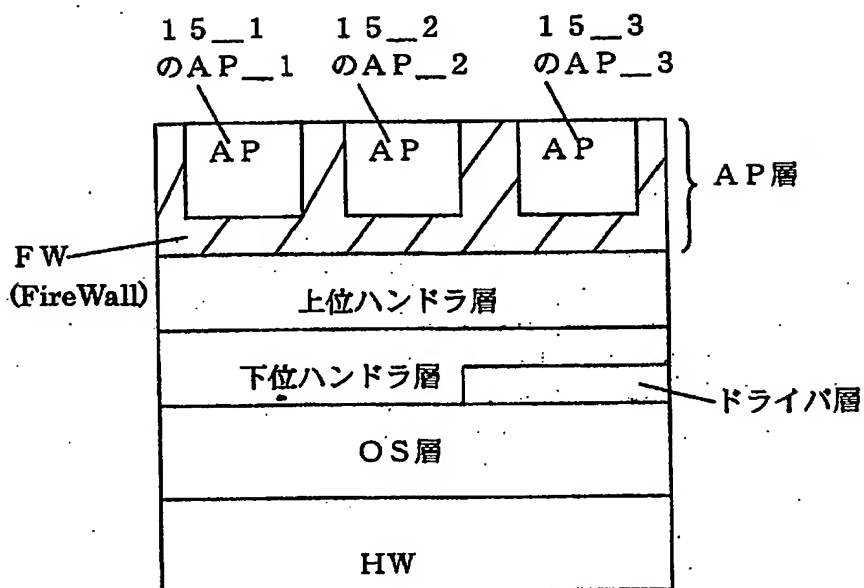
【図5】



【図6】



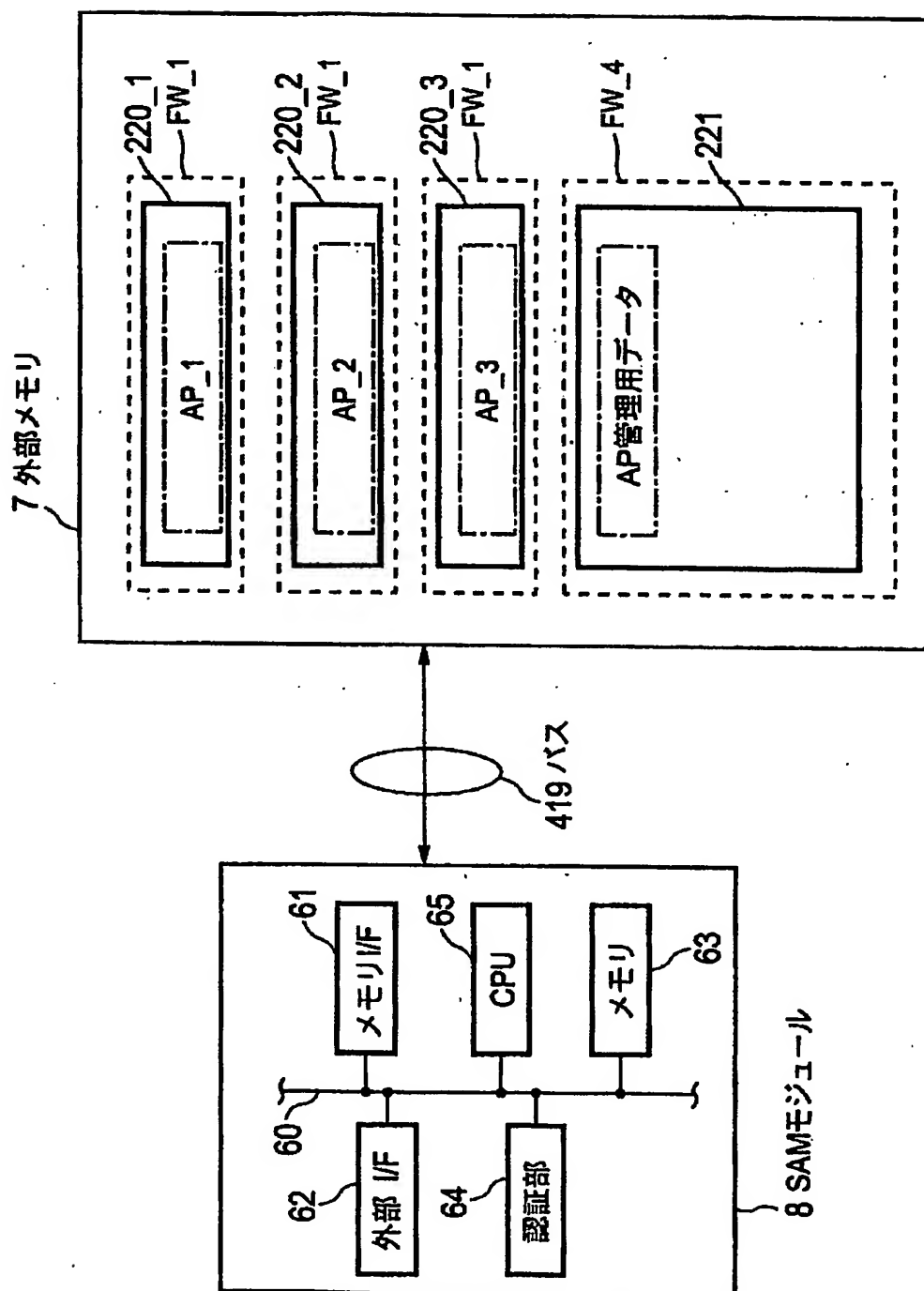
【図7】



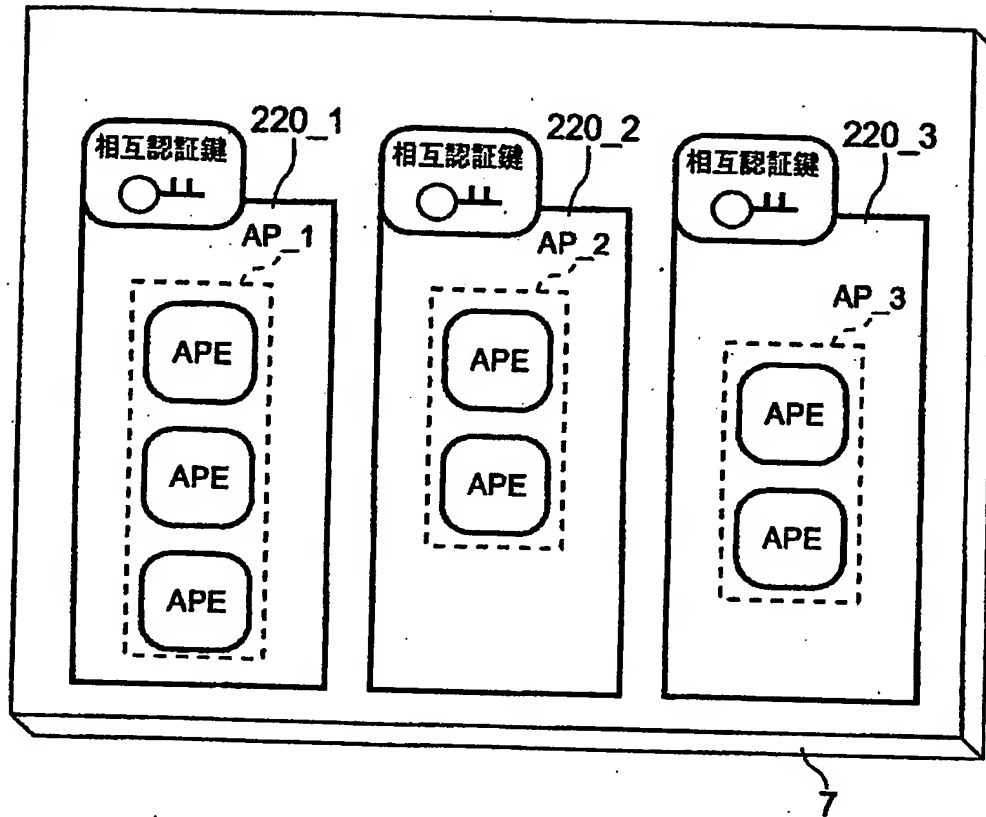
SAMモジュールのソフトウェア構成



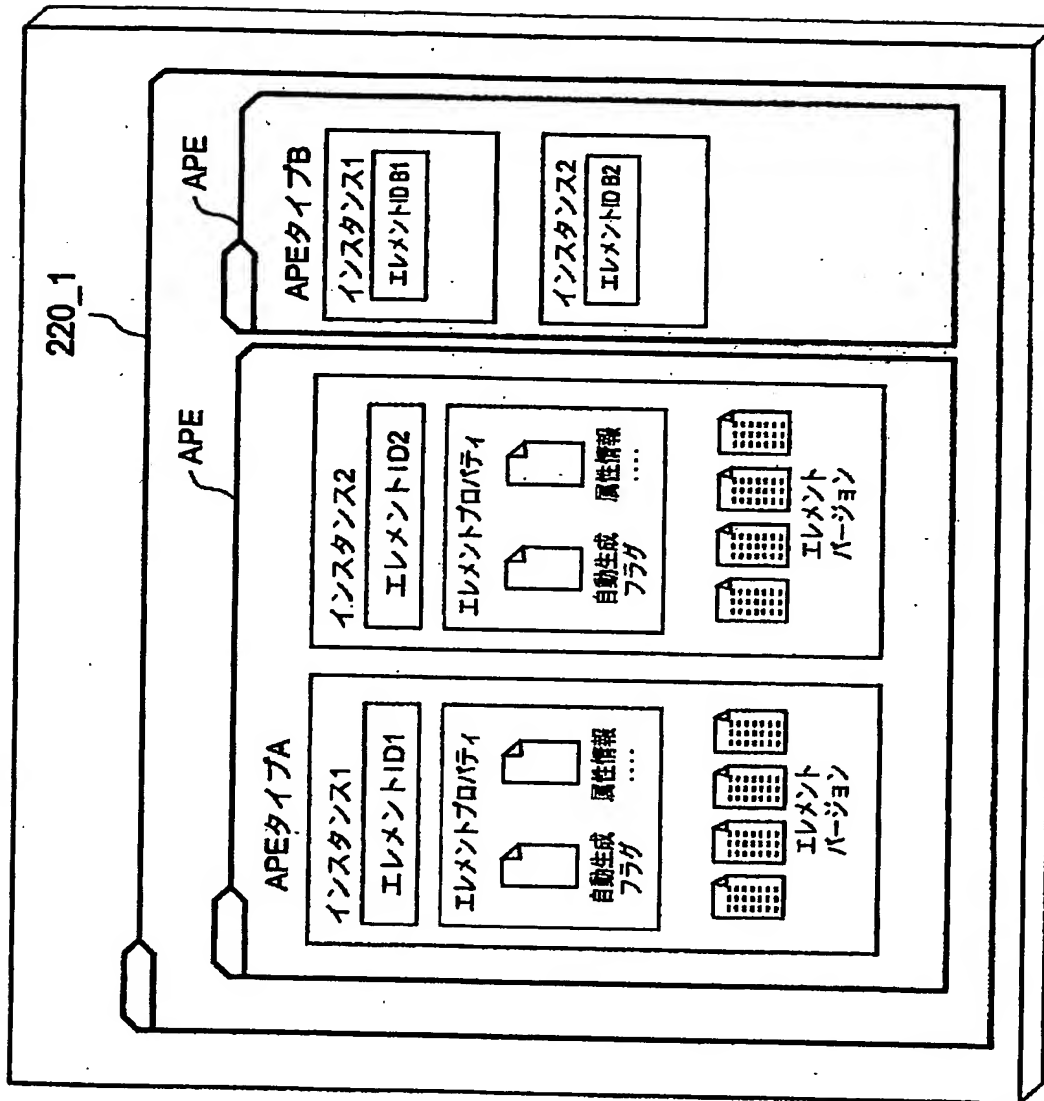
【図8】



【図9】



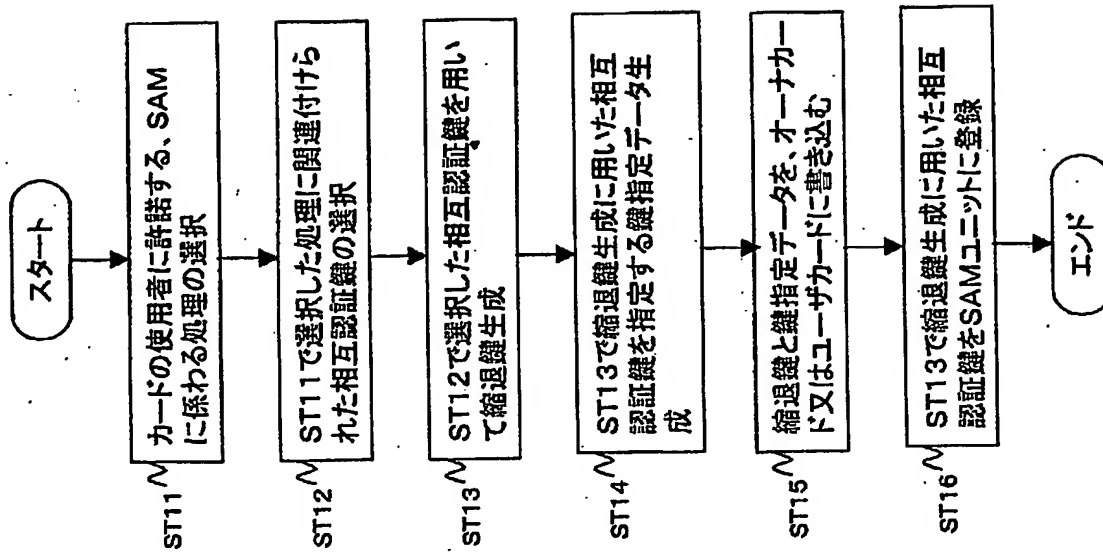
【図10】



【図 11】

APE タイプ番号	APEタイプ
...	ICシステム鍵
...	ICエリア鍵
...	ICサービス鍵
...	IC縮退鍵
...	IC鍵変更パッケージ
...	IC発行鍵パッケージ
...	IC拡張発行鍵パッケージ
...	ICエリア登録鍵パッケージ
...	ICエリア削除鍵パッケージ
...	ICサービス登録鍵パッケージ
...	ICサービス削除鍵パッケージ
...	ICメモリ分割鍵パッケージ
...	ICメモリ分割素鍵パッケージ
...	障害記録ファイル
...	相互認証用鍵
...	パッケージ鍵
...	ネガリスト
...	サービスデータテンポラリファイル

【図 12】



【図 13】

相互認証鍵名	AP記憶領域・ID	APEタイプ 番号	インスタンス 番号	エレメント バージョン
デバイス鍵	...	...	...	...
ターミネーション鍵	...	...	...	...
製造設定サービス相互認証鍵	...	...	...	...
機器管理サービス相互認証鍵	...	...	...	...
通信管理サービス相互認証鍵	...	...	...	...
相互認証サービス相互認証鍵	...	...	...	...
AP記憶領域管理サービス 相互認証鍵	...	...	...	...
サービスAP・記憶領域 相互認証鍵	...	...	...	...
システムAP・記憶領域 相互認証鍵	...	...	...	...
製造者AP記憶領域 相互認証鍵	...	...	...	...

【図 14】

AP記憶領域ID	エレメントタイプ番号	エレメント インスタンス番号	エレメント バージョン番号
2バイト	2バイト	2バイト	2バイト
所属する APリソース領域	相互認証鍵 (固定値)	リリース鍵リングのID	使用する鍵の バージョン番号

相互認証コード

【図 1 5】

相互認証鍵名	AP記憶領域ID	APE タイプ番号	インスタンス 番号	エレメント バージョン番号
デバイス鍵	...	...	...	...
機器管理サービス相互認証鍵	...	...	...	...
通信管理サービス相互認証鍵	...	...	...	...
AP記憶領域管理サービス 相互認証鍵	...	...	...	...
サービスAP記憶領域 AP-R相互認証鍵	...	...	...	...
ターミネーション鍵	...	...	...	...

(A)

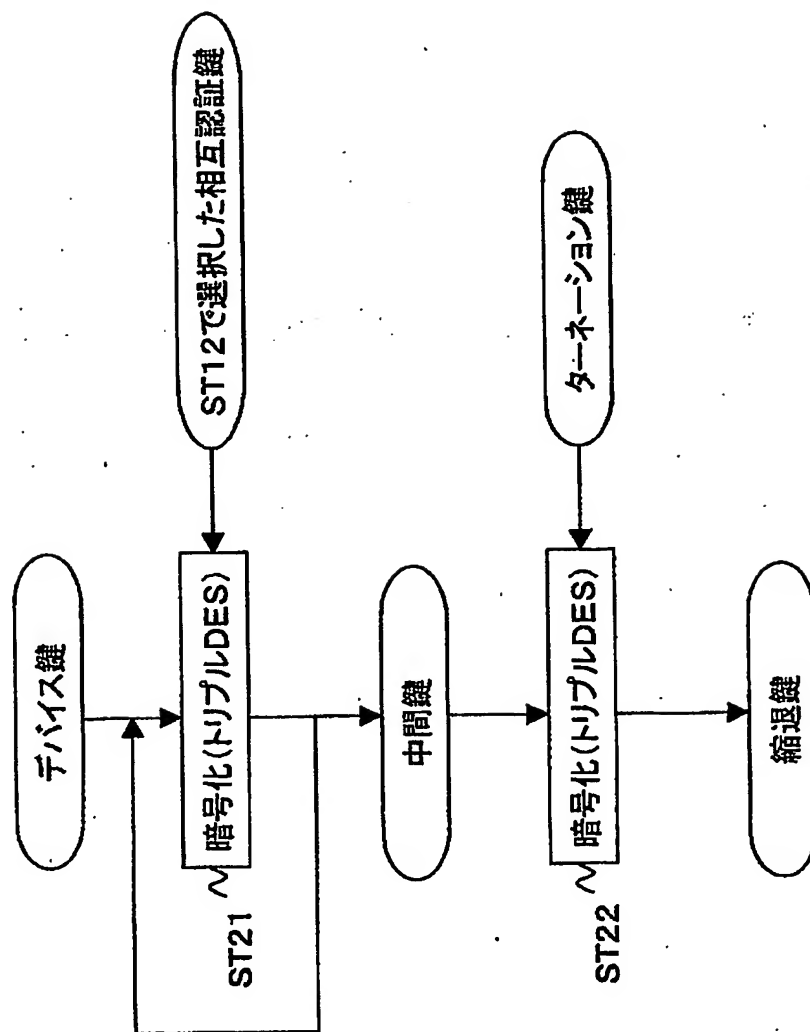
・実行可能なコマンド

サービス種別	コマンド名
機器管理サービス	...
通信管理サービス	...
ICサービス	...
相互認証サービス	...
AP記憶領域管理サービス	...

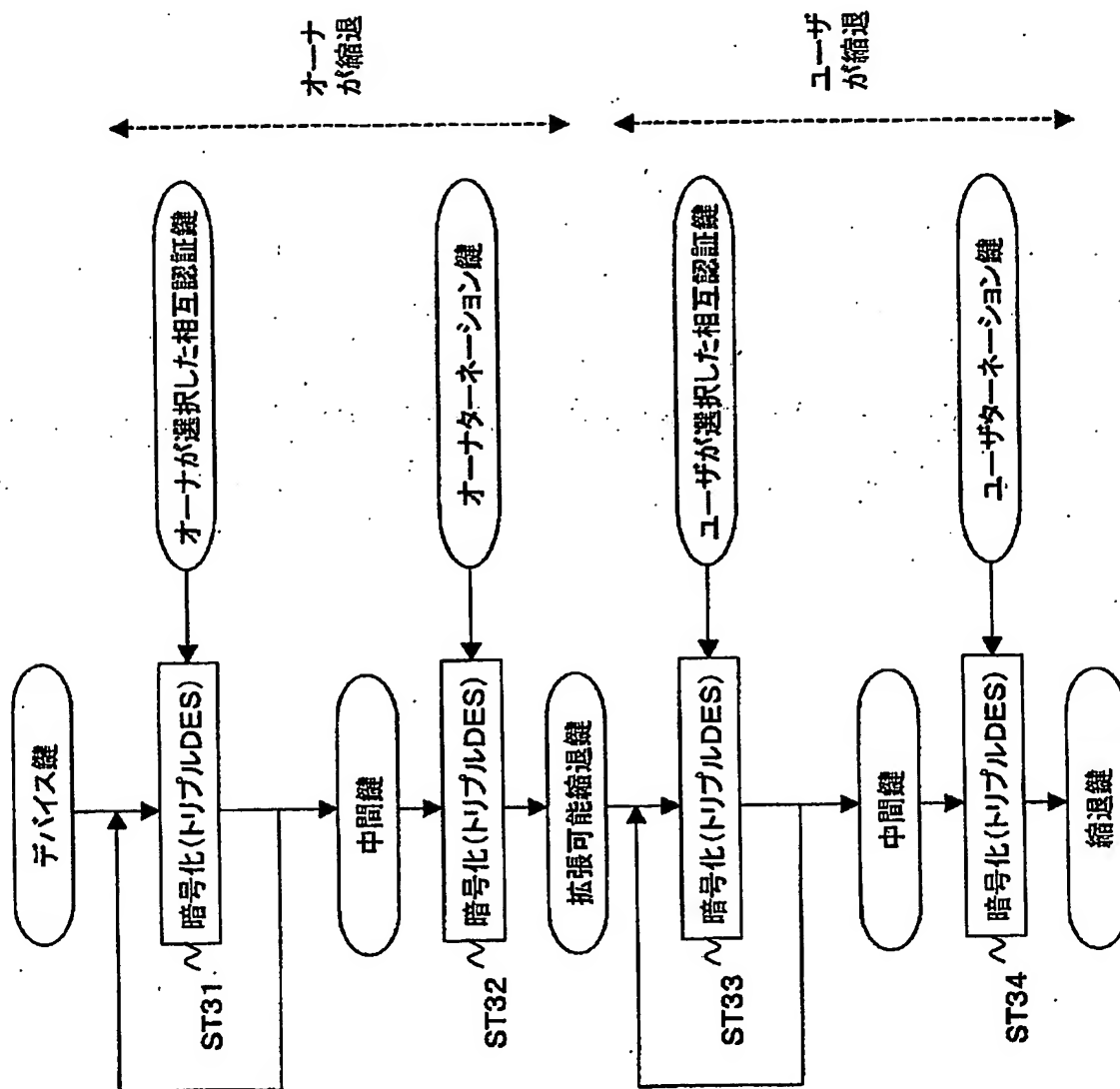
(B)



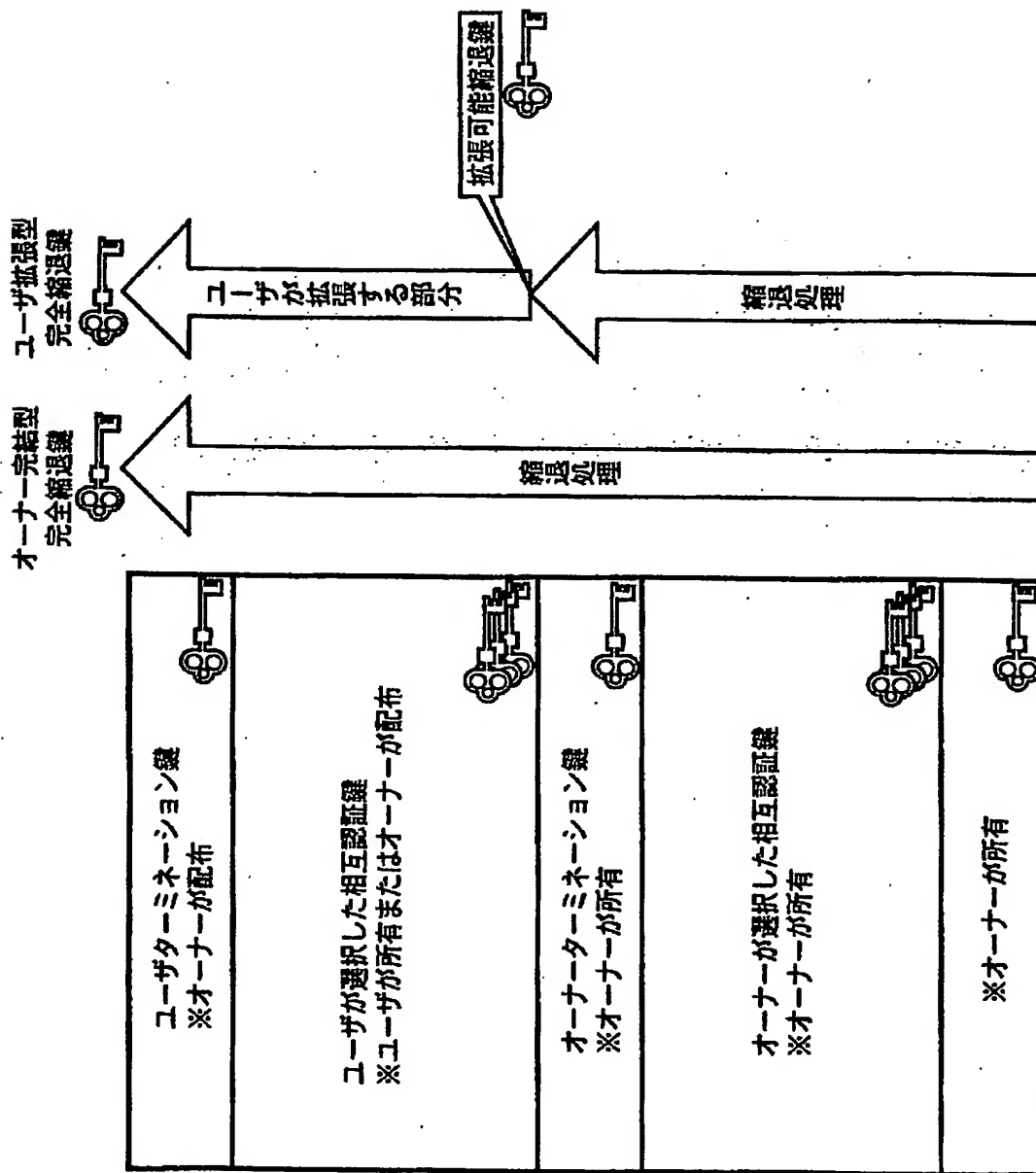
【図 16】



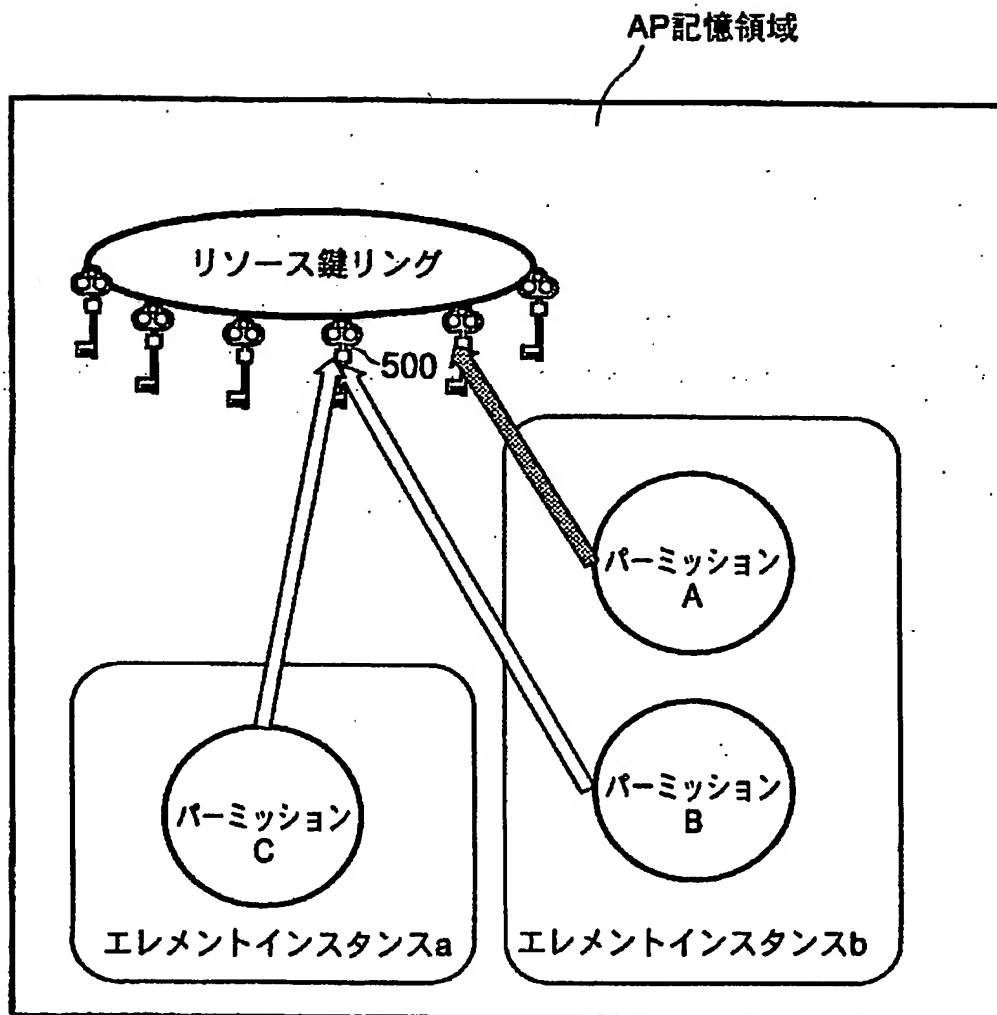
【図17】



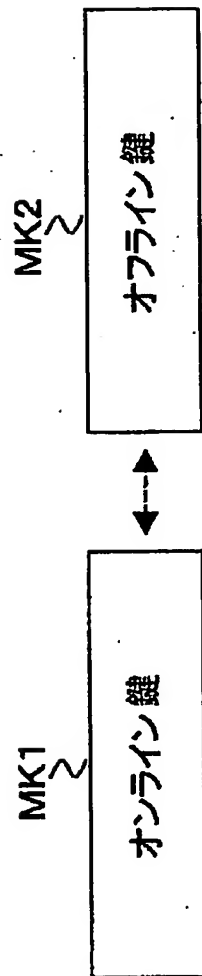
【図18】



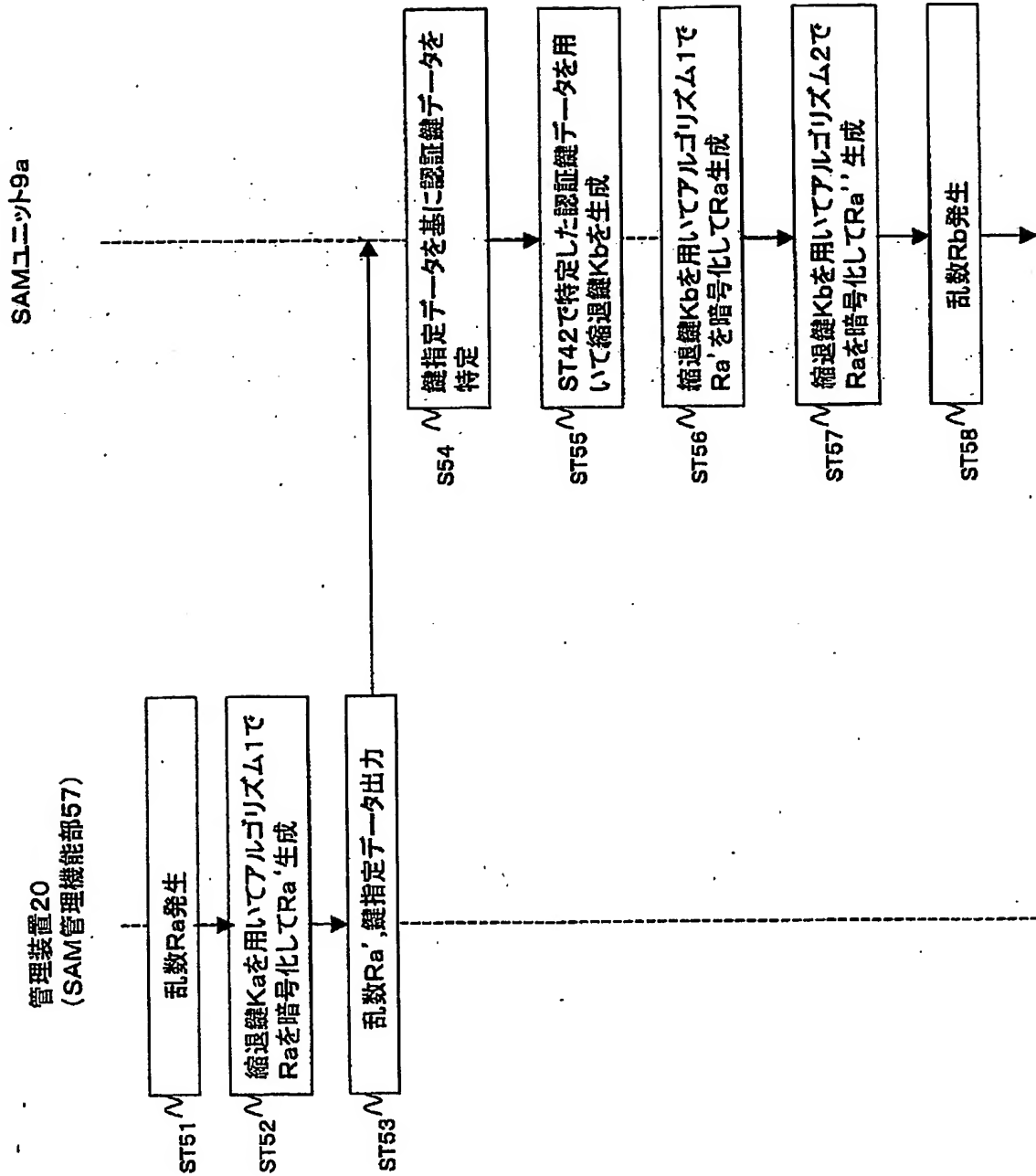
【図19】



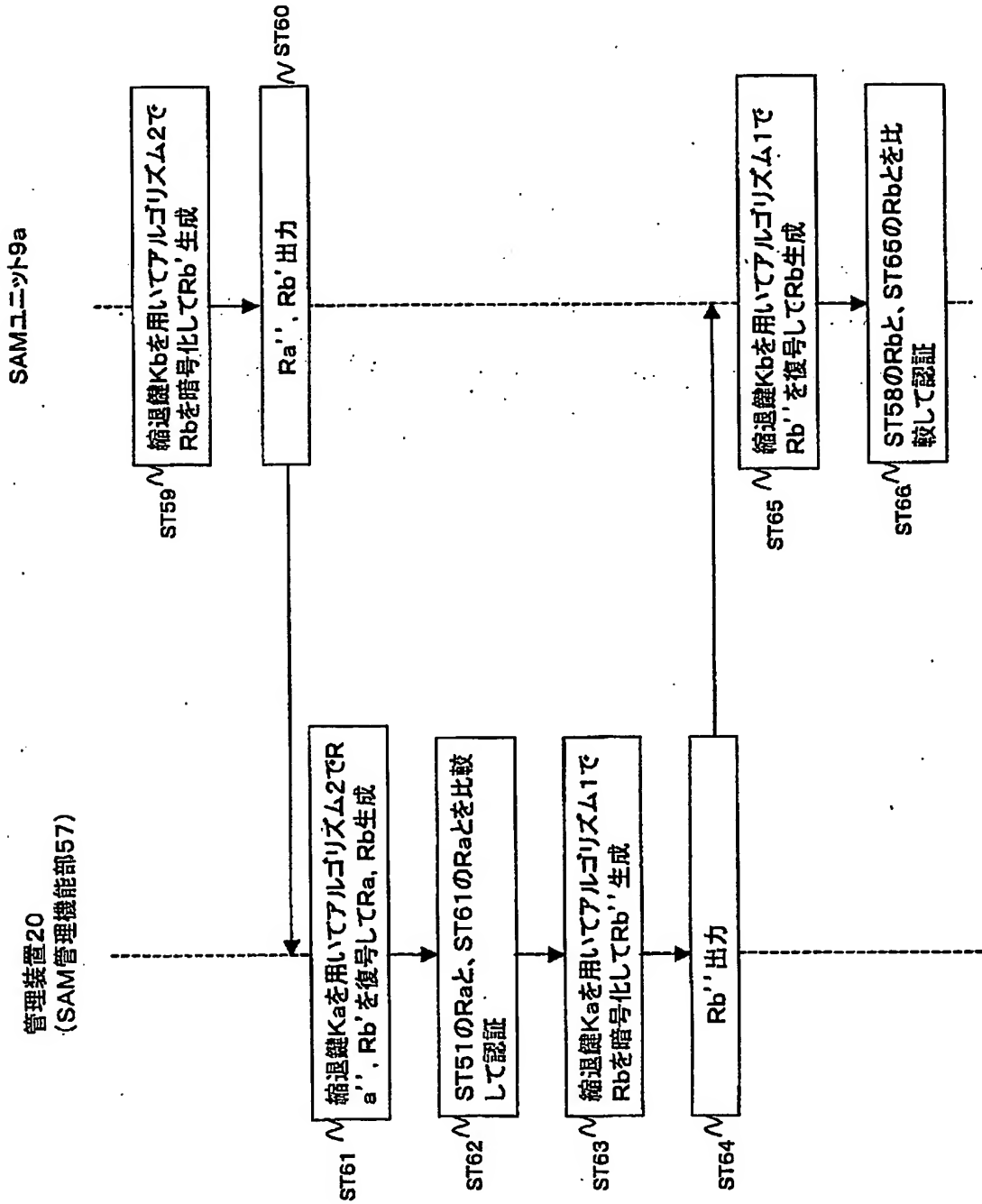
【図 20】



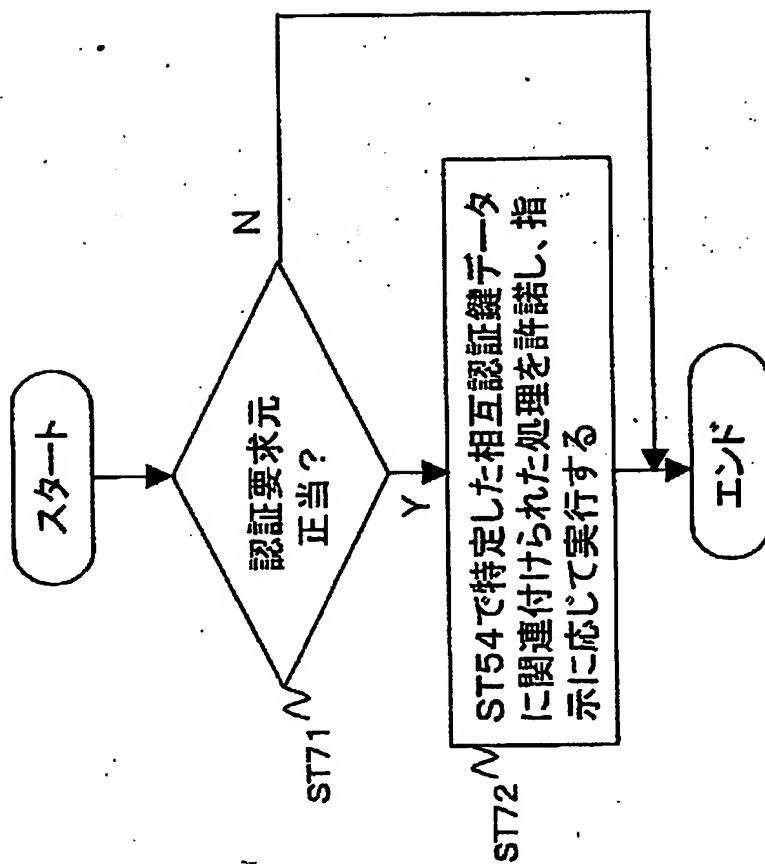
【図 21】



【図 22】

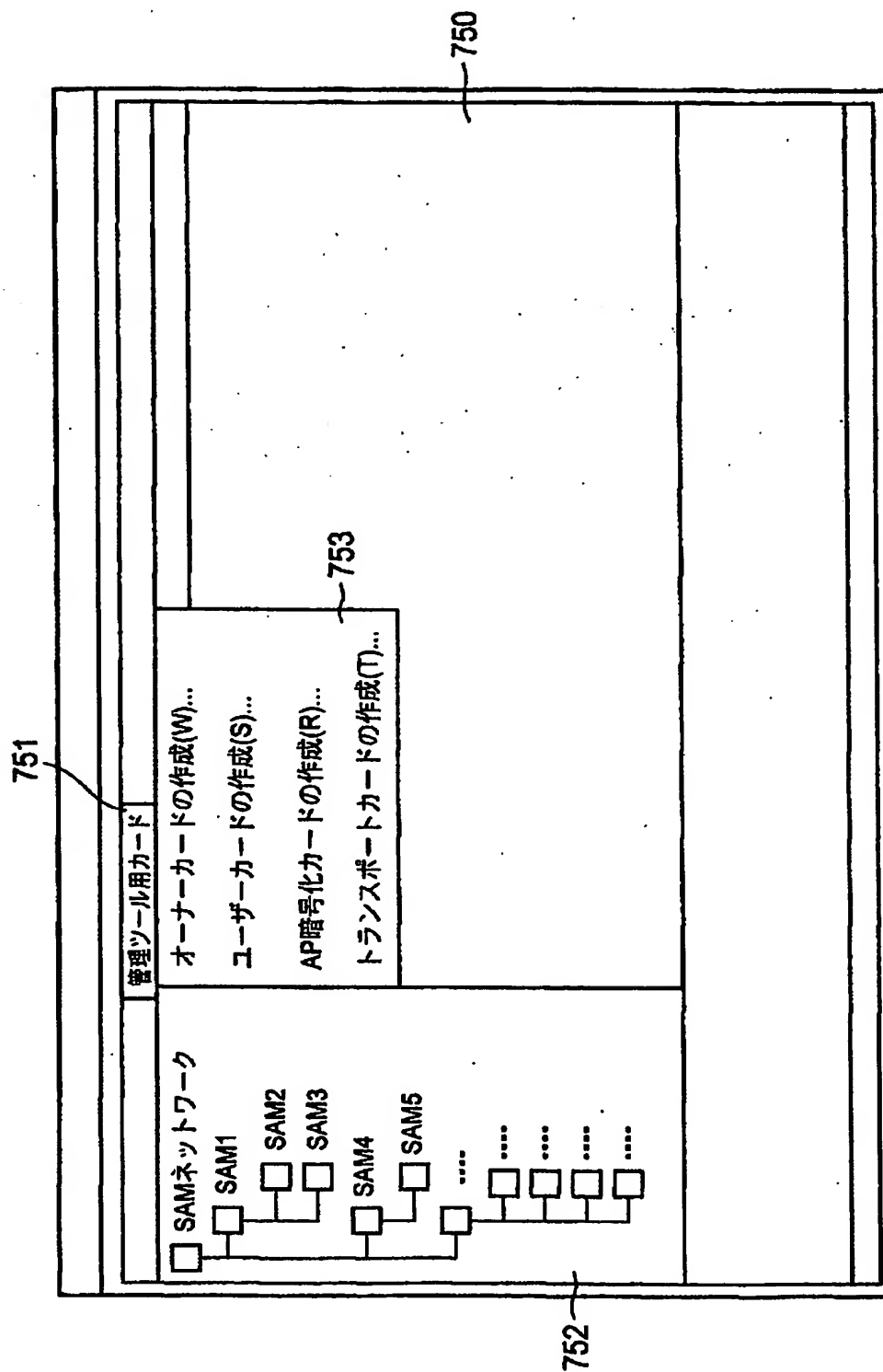


【図 23】





【図 24】



【図 25】

オーナーカードの作成

利用サービスの選択

<input checked="" type="checkbox"/> 機器管理サービス	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> 通信管理サービス	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> 相互認証サービス	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> APリソース領域管理サービス	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> ログ記録サービス	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> ネガリストサービス	鍵バージョン: 0x0001 ▼

サービスAP記憶領域

<input checked="" type="checkbox"/> 読み取り	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> 書き込み	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> パッケージ	鍵バージョン: 0x0001 ▼

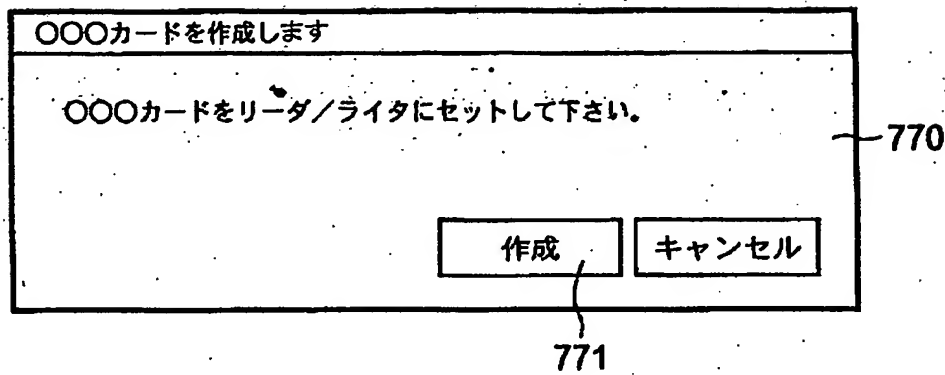
システムAP記憶領域

<input checked="" type="checkbox"/> 読み取り	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> 書き込み	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> パッケージ	鍵バージョン: 0x0001 ▼

デバイス/ターミネーション鍵

<input checked="" type="checkbox"/> デバイス鍵	鍵バージョン: 0x0001 ▼
<input checked="" type="checkbox"/> ターミネーション鍵	鍵バージョン: 0x0001 ▼

【図 26】



【図 27】

ユーザカードの作成

781

利用サービスの選択

☐ 機器管理サービス 鍵バージョン: 0x0001 ▼

☒ 通信管理サービス 鍵バージョン: 0x0001 ▼

☒ 相互認証サービス 鍵バージョン: 0x0001 ▼

☒ APリソース領域管理サービス 鍵バージョン: 0x0001 ▼

☐ ログ記録サービス 鍵バージョン: 0x0001 ▼

☐ ネガリストサービス 鍵バージョン: 0x0001 ▼

780

サービスAP記憶領域

☐ 読み取り 鍵バージョン: 0x0001 ▼

☐ 書き込み 鍵バージョン: 0x0001 ▼

☒ パッケージ 鍵バージョン: 0x0001 ▼

782

システムAP記憶領域

☒ 読み取り 鍵バージョン: 0x0001 ▼

☒ 書き込み 鍵バージョン: 0x0001 ▼

☒ パッケージ 鍵バージョン: 0x0001 ▼

783

デバイス/ターミネーション鍵

☒ デバイス鍵 鍵バージョン: 0x0001 ▼

☒ ターミネーション鍵 鍵バージョン: 0x0001 ▼

784

OK キャンセル

785

【図 28】

APリソース暗号化カードの作成

790

利用サービスの選択

791

機器管理サービス 鍵バージョン: 0x0001 ▼

通信管理サービス 鍵バージョン: 0x0001 ▼

相互認証サービス 鍵バージョン: 0x0001 ▼

APリソース領域管理サービス 鍵バージョン: 0x0001 ▼

ログ記録サービス 鍵バージョン: 0x0001 ▼

ネガリストサービス 鍵バージョン: 0x0001 ▼

サービスAP記憶領域

792

読み取り 鍵バージョン: 0x0001 ▼

書き込み 鍵バージョン: 0x0001 ▼

パッケージ 鍵バージョン: 0x0001 ▼

システムAP記憶領域

793

読み取り 鍵バージョン: ▼

書き込み 鍵バージョン: ▼

パッケージ 鍵バージョン: ▼

デバイス/ターミネーション鍵

794

デバイス鍵 鍵バージョン: ▼

ターミネーション鍵 鍵バージョン: ▼

OK キャンセル

795

【図 29】

トランスポートカードの作成

次のAPリソースエレメントを読み出します。

SAM IPアドレス: . . .

AP記憶領域: サービス領域 ▼

エレメントタイプ: IC分割鍵 ▼

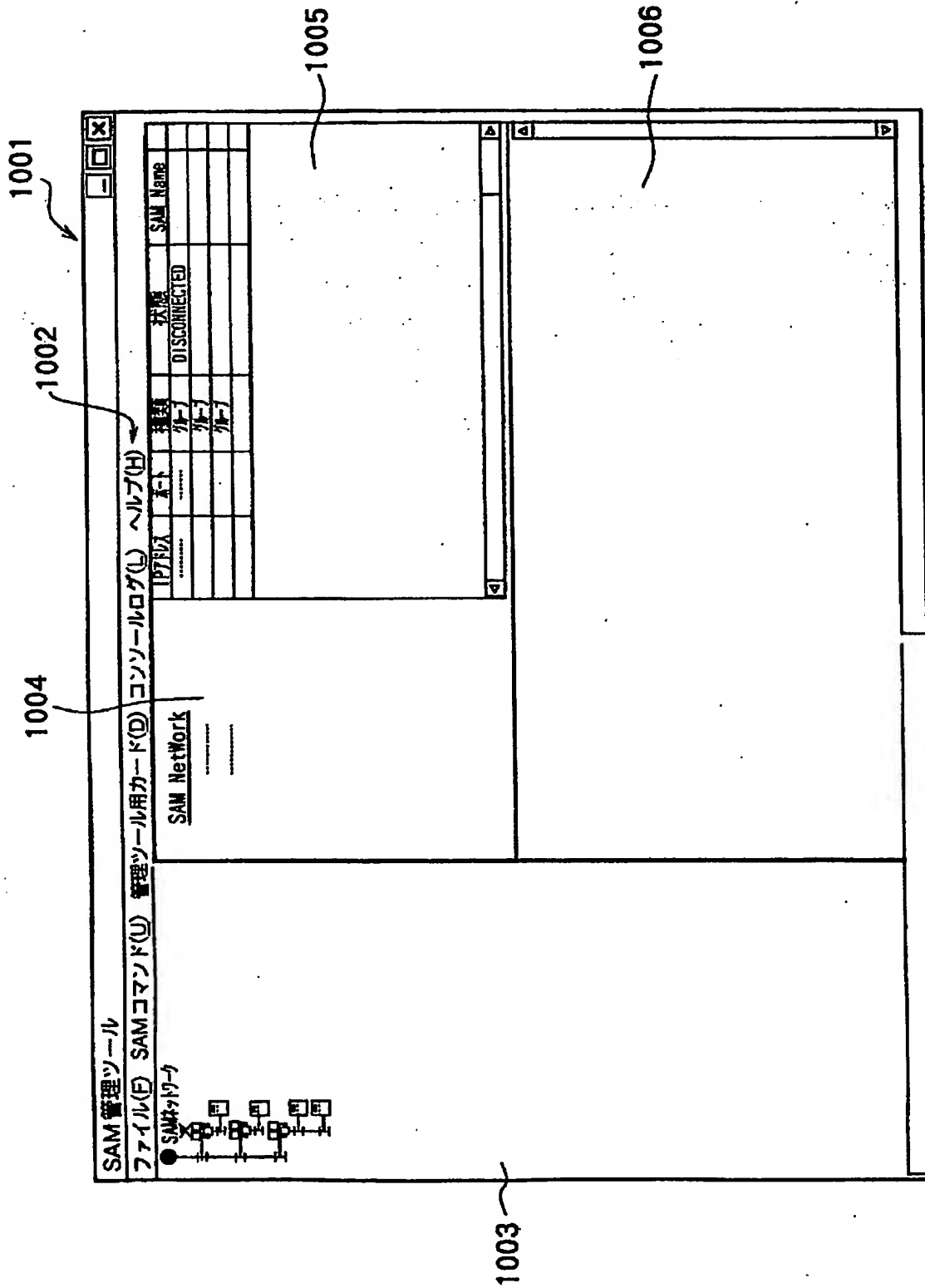
インスタンス番号: 0000h ▼

バージョン: 0000h ▼

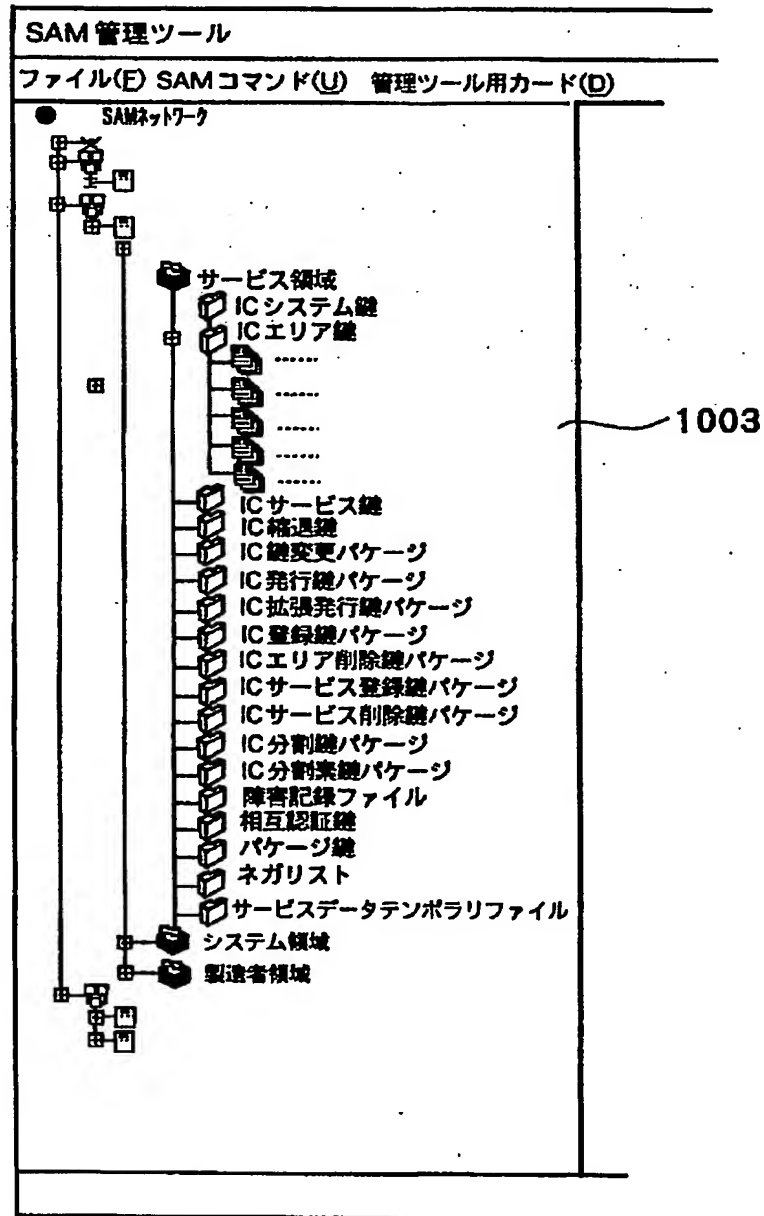
OK キャンセル

800

【図30】

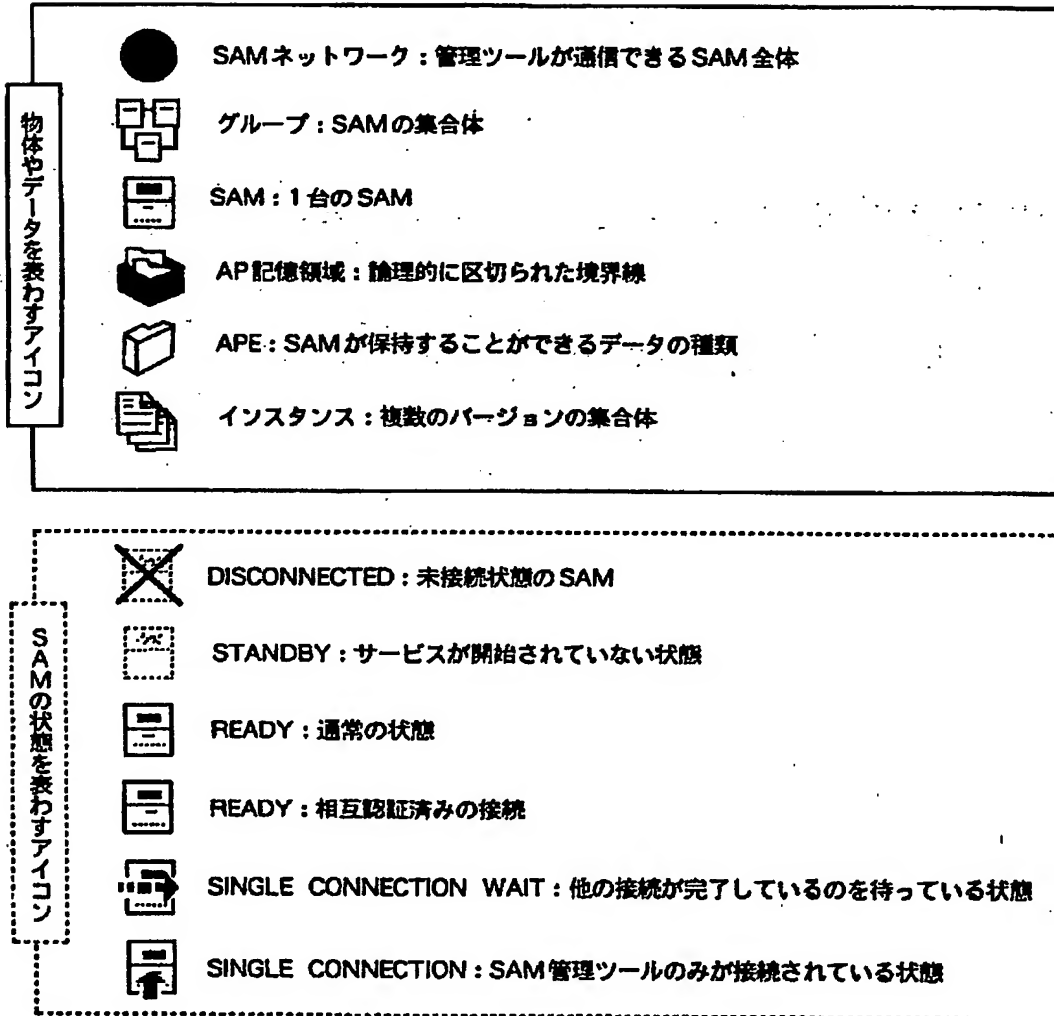


【図 31】





【図 3 2】



【図 33】

コンソールログ(L) ヘルプ(H)					
SAM Network					
IPアドレス	ポート	種類	状態	SAM Name	サイト
*****	*****	SAM			
		11-7			
		11-7			
		11-7			

1010

【図 34】

IPアドレス	ホスト	種類	状態	SAM Name	エイット
.....	.....	SAM	READY		

Group

1020

【図 35】

コンソールログ(L) ヘルプ(H)		種類	用途
SAM READY-F	記憶領域	AP記憶領域	AP記憶領域
	*****	AP記憶領域	AP記憶領域
	*****	AP記憶領域	AP記憶領域
	*****	AP記憶領域	製造者領域

1030

【図 36】

AP Resource Partition	
サービス領域	
APEタイプ番号	APEタイプ
	システム鍵
	ICエリア鍵
	ICサービス鍵
	IC秘通鍵
	IC鍵変更パッケージ
	IC発行鍵パッケージ
	IC秘通発行鍵パッケージ
	IC登録鍵パッケージ
	ICエリア削除鍵パッケージ
	ICサービス登録鍵パッケージ
	ICサービス削除鍵パッケージ
	IC分割鍵パッケージ
	IC分割鍵パッケージ
	障害記録ファイル
	相互認証鍵
	パッケージ鍵
	ネガリスト
	サービスデータテンポラリファイル

1040

【図 3 7】

[illegible]

1050

【図 38】

1060

Instance
SAH-EVT-33

.....

.....:jp

READY-カード

カード領域

ICカード

カード番号:.....

最大Ver:.....

使用Ver:.....

最小Ver:.....

最大Ver:.....

有効:.....

自動生成:はい

エラー取得:可能

削除:可能

カード:.....

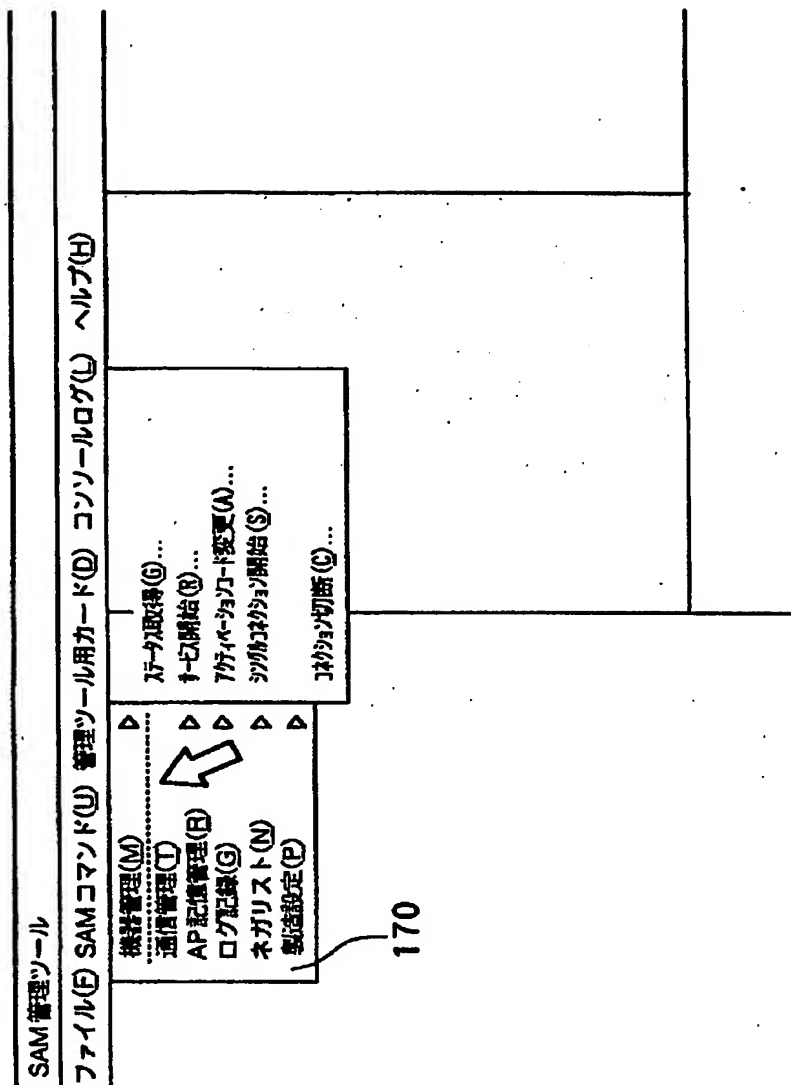
カード:.....

現在カード:.....

37

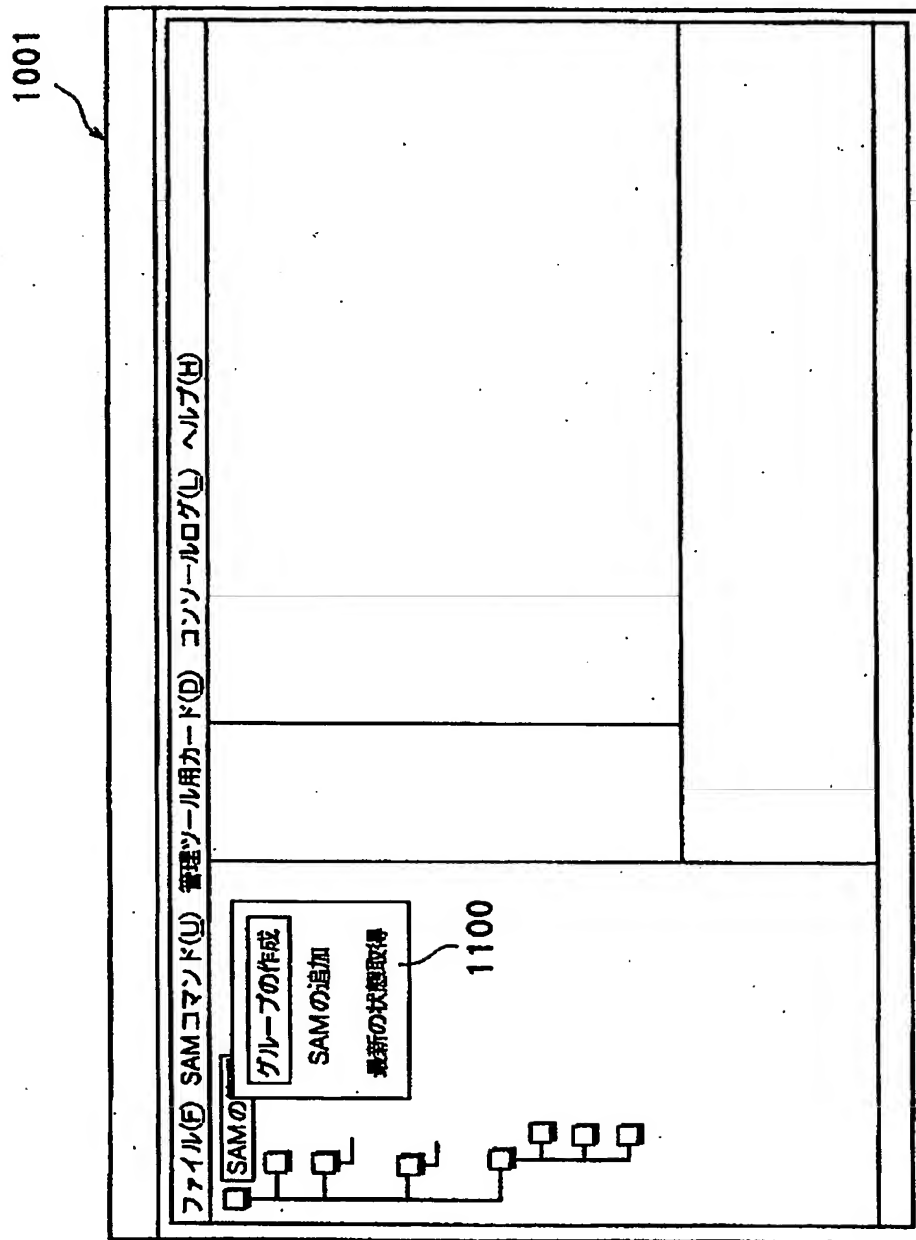
出証特 2003-3047701

【図 39】

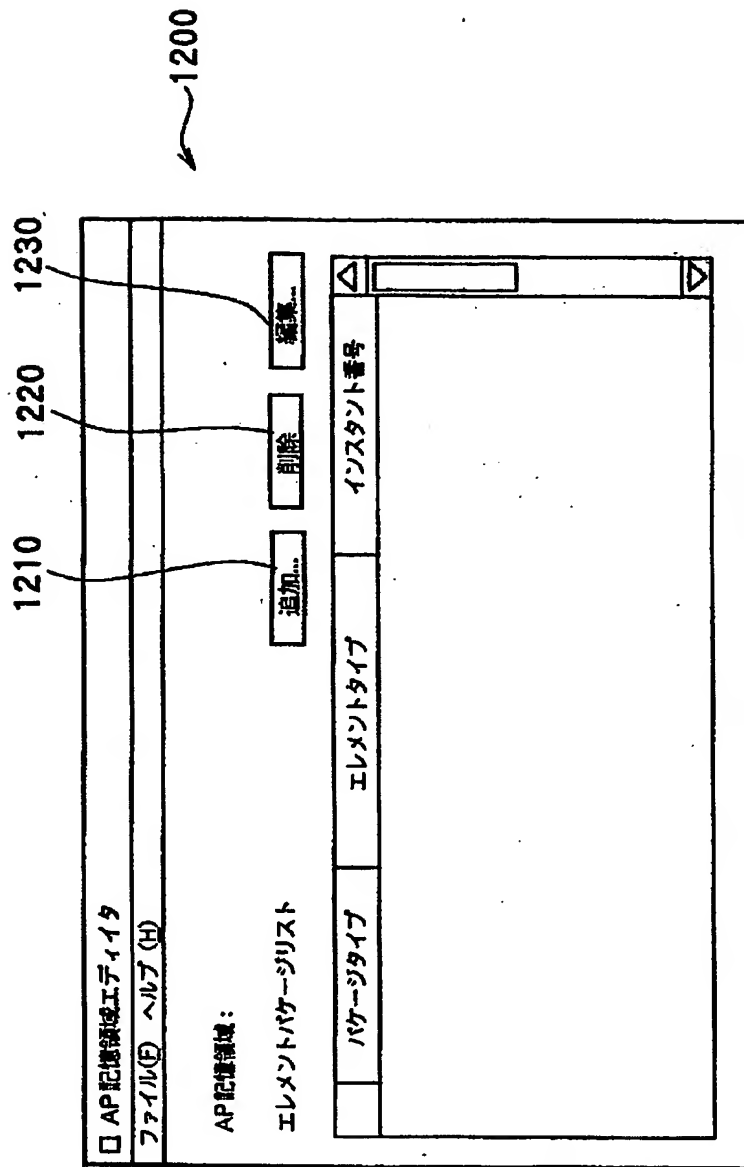




【図 40】



【図 41】



【図 4 2】

エレメントパッケージの追加

エレメントパッケージタイプ

☒ エレメント作成 1301

☐ パッケージ追加

APEタイプ: ICシステム 1302

インスタンス番号: 1303

ファイル... OK キャンセル 1304

1300

【図 43】

APE作成

エレメントタイプ: ICシステム鍵      インスタンス番号: .....

タグ:  データ自動生成: ☐ 可 ☐ 可

使用バージョン数:  エレメント削除: ☐ 可 ☐ 可

エレメント取得: ☐ 可 ☐ 不可 カード参照...

属性情報

属性情報名	値
システムコード	<input type="text" value="1406"/>

属性編集...      保存      キャンセル

【図 44】

APEバージョン追加

エレメントタイプ: IC 變更パッケージ インスタンス番号: .....

エレメントバージョン:  總データ入力方法:  ▽

エレメントデータ

項目名	値
IC 變更パッケージ	XXX...

【図 45】

□ AP 記憶領域エディタ

ファイル(F) ヘルプ(H)

AP 記憶領域: サービス領域

エレメントパッケージリスト

追加... 削除 編集...

	パッケージタイプ	エレメントタイプ	インスタント番号
1	エレメント作成	IC サービス領域	.....
2	パッケージ追加	IC サービス領域	.....
3	エレメント作成	IC サービス領域	.....
4	パッケージ追加	IC サービス領域	.....

120

1240

【書類名】 要約書

【要約】

【課題】 認証手段が被認証手段を認証した後に、当該被認証手段に許可した処理を実行する場合に、認証手段の処理負担を軽減することを可能にするデータ処理方法を提供する。

【解決手段】 管理装置20が、カードから読み込んだ鍵指定データをSAMユニットに9aに出力する。SAMユニット9aが、鍵指定データが指定する相互認証鍵データを用いて縮退鍵データを生成する。管理装置20とSAMユニット9aとで縮退鍵データを用いて認証を行う。SAMユニット9aが管理装置20の正当性を認めると、上記縮退鍵データの生成に用いられた単数または複数の相互認証鍵データに関連付けられた処理を実行する。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社
2. 変更年月日 2003年 5月15日  
[変更理由] 名称変更  
住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社